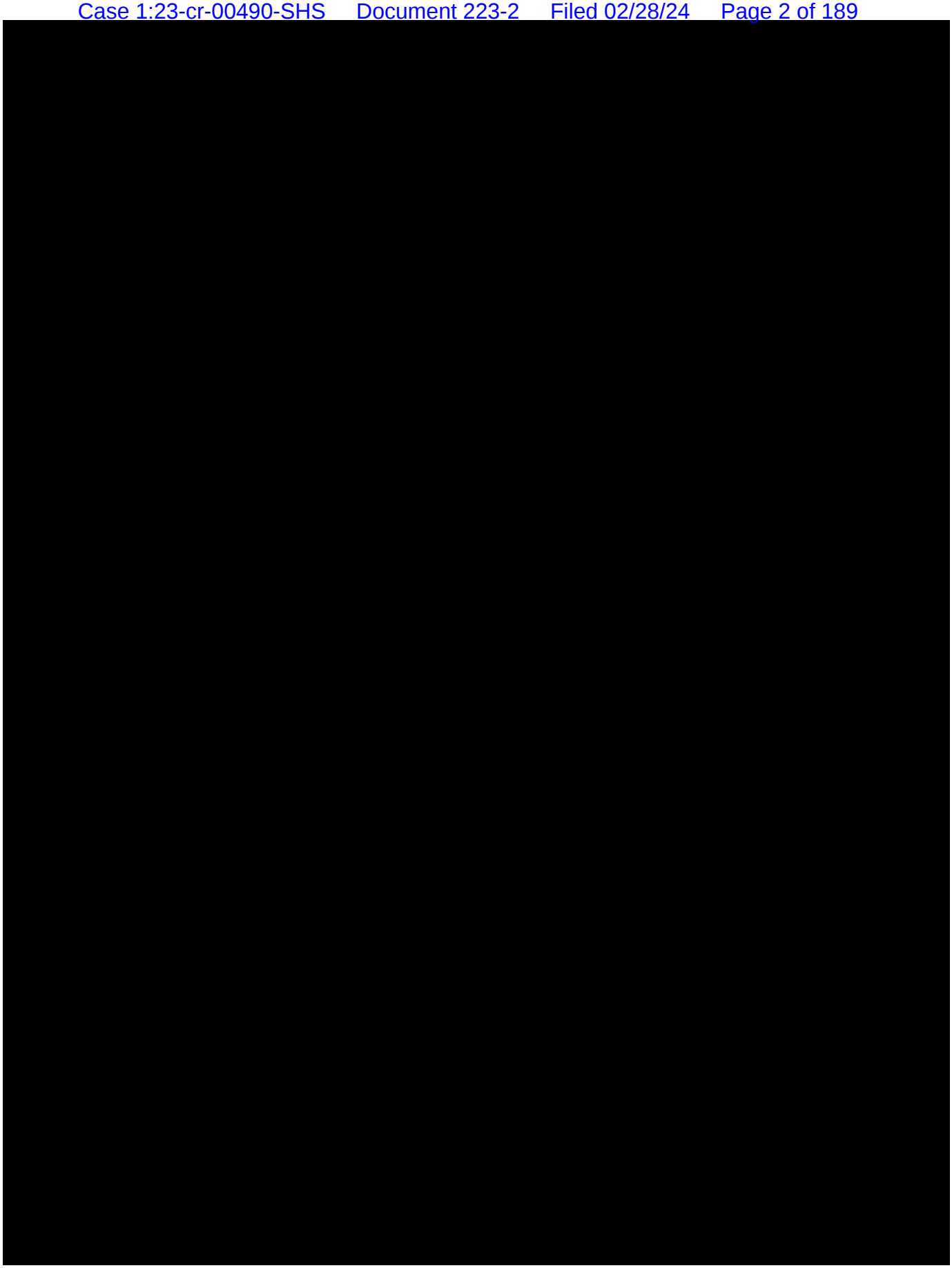
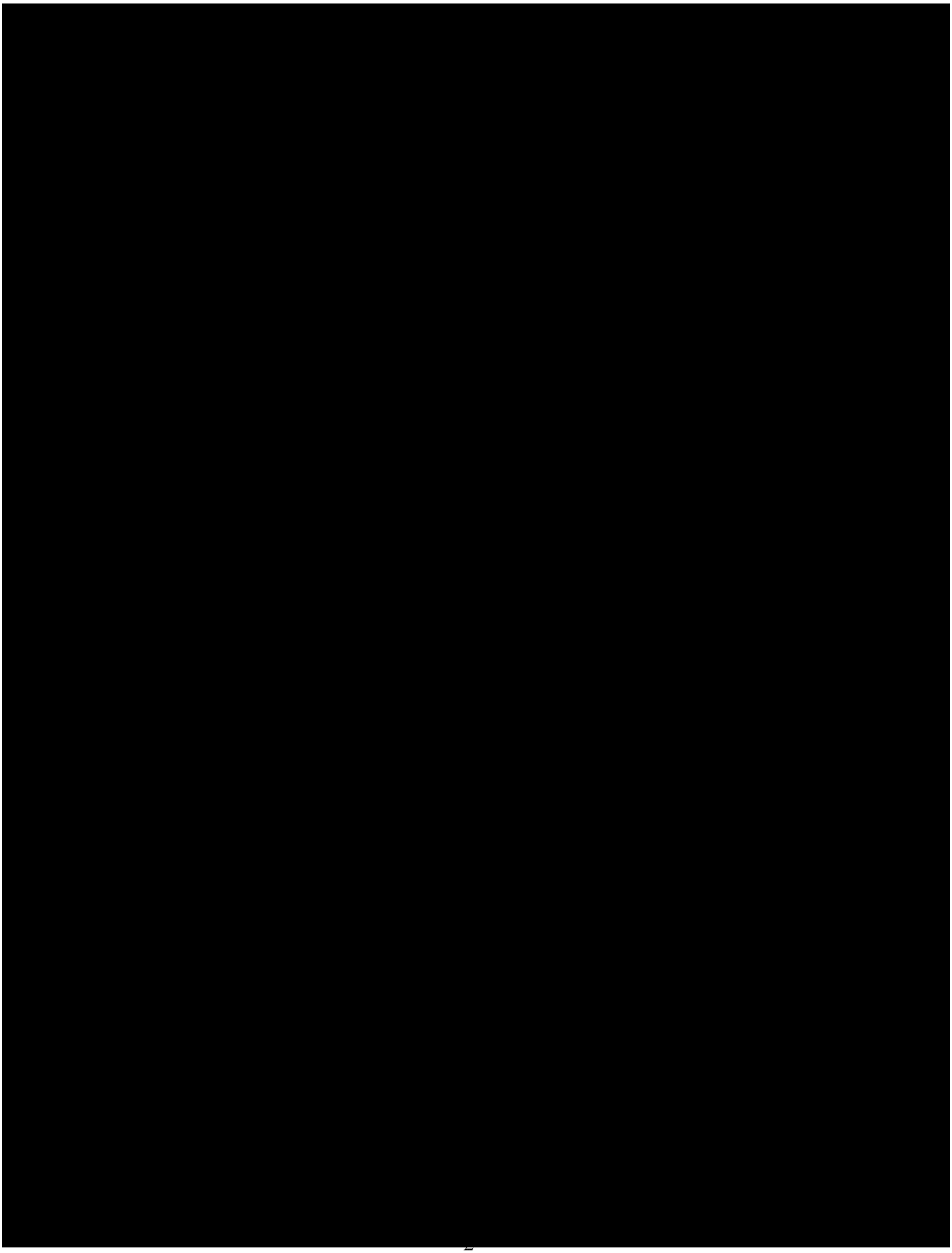
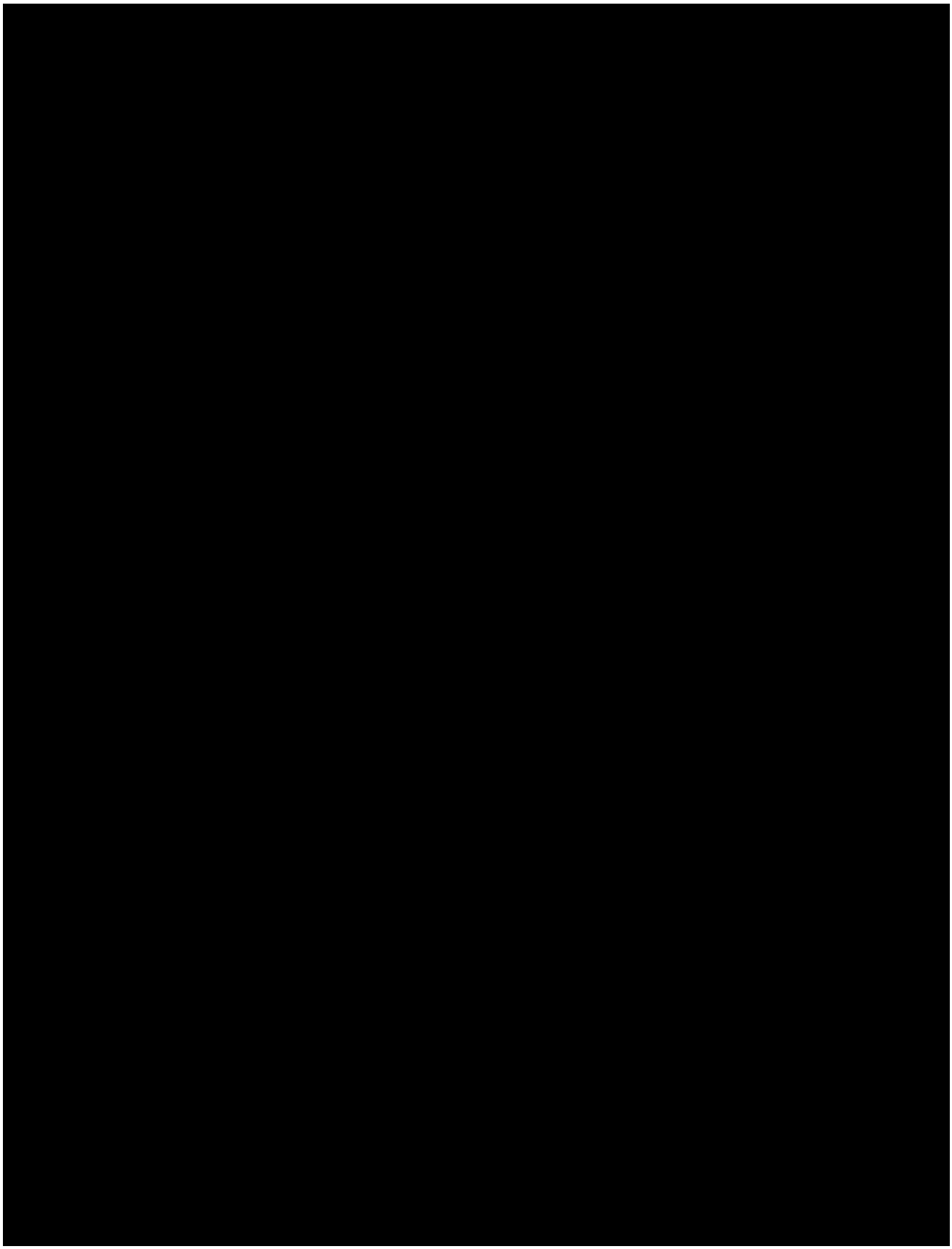
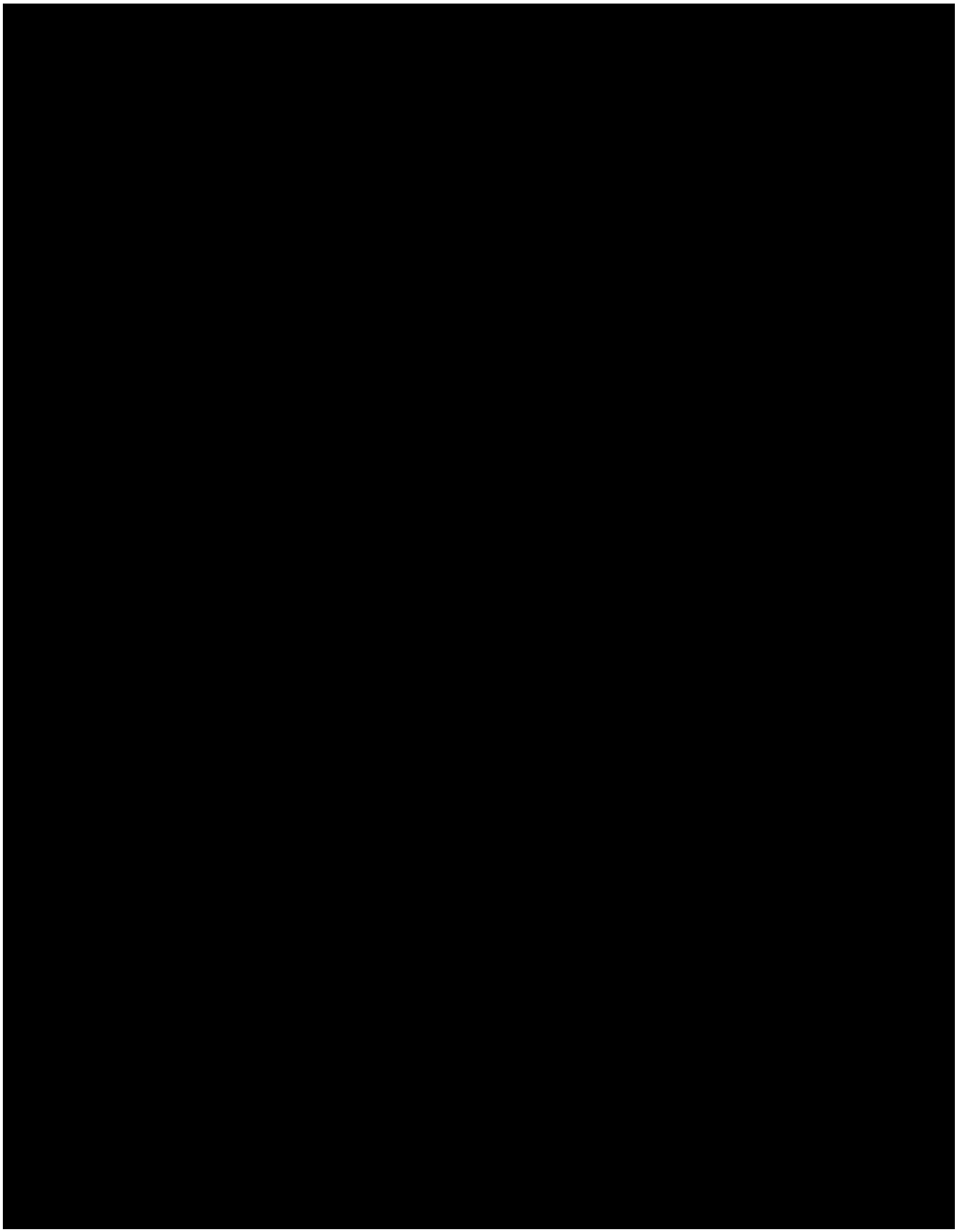
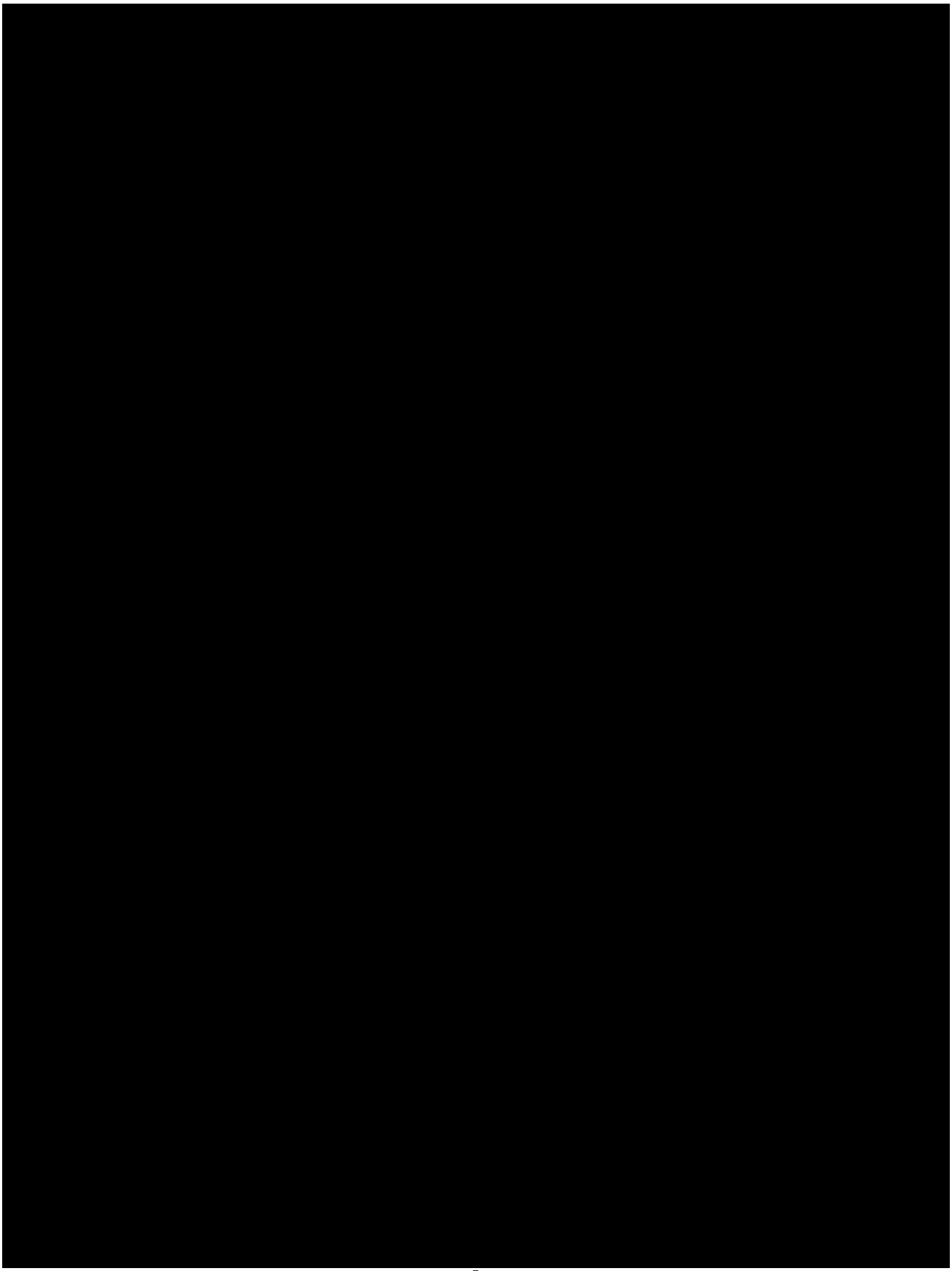
EXHIBIT B

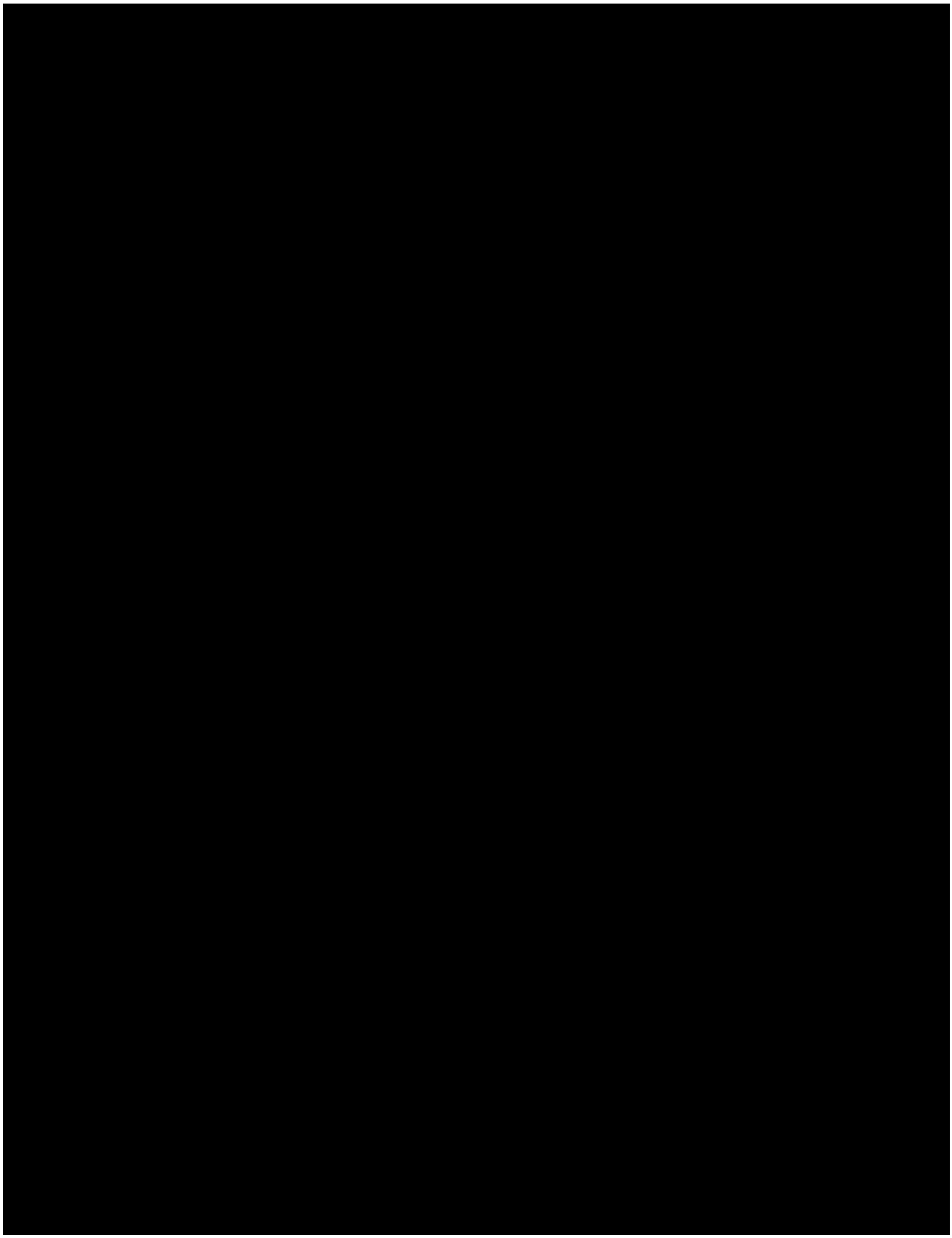


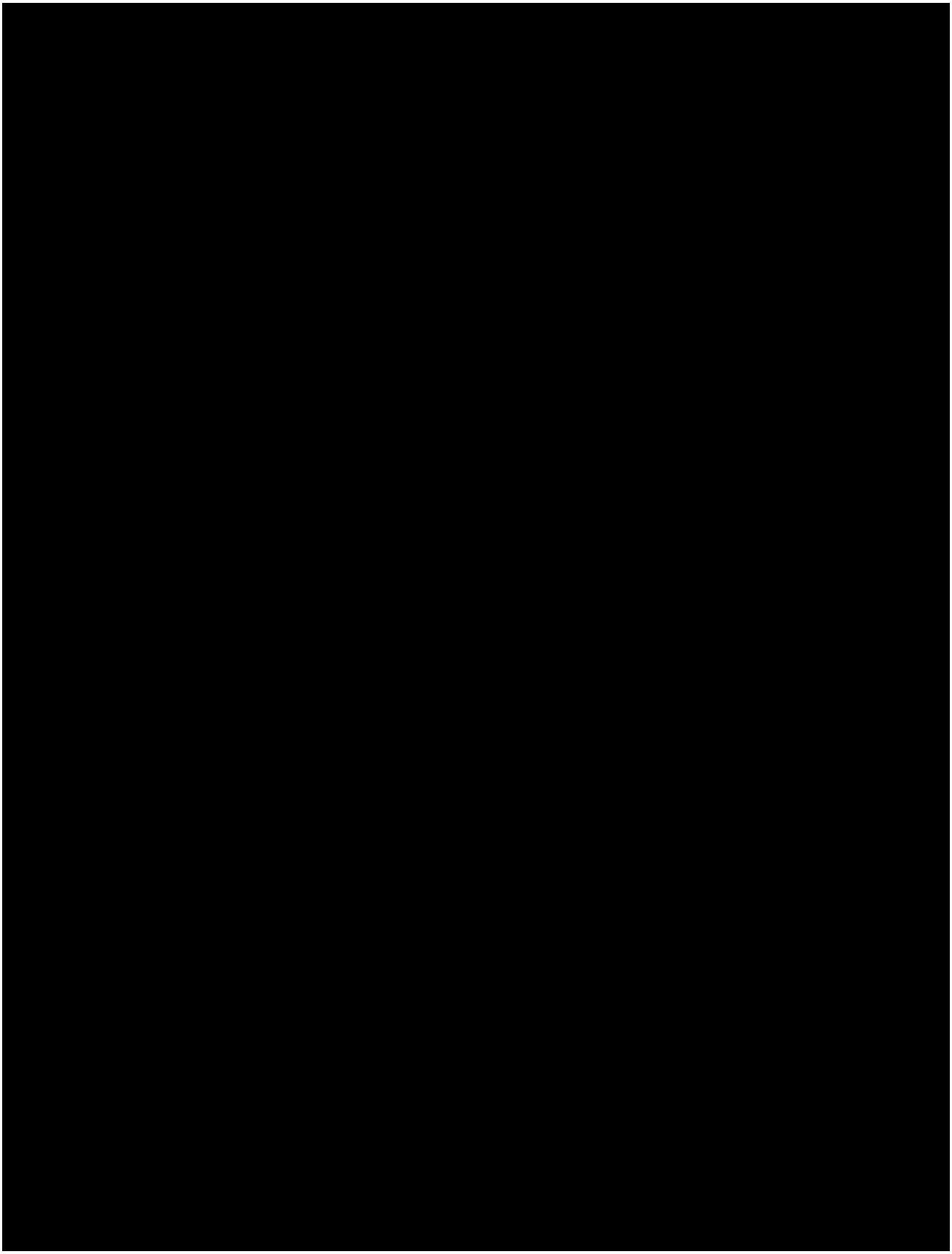


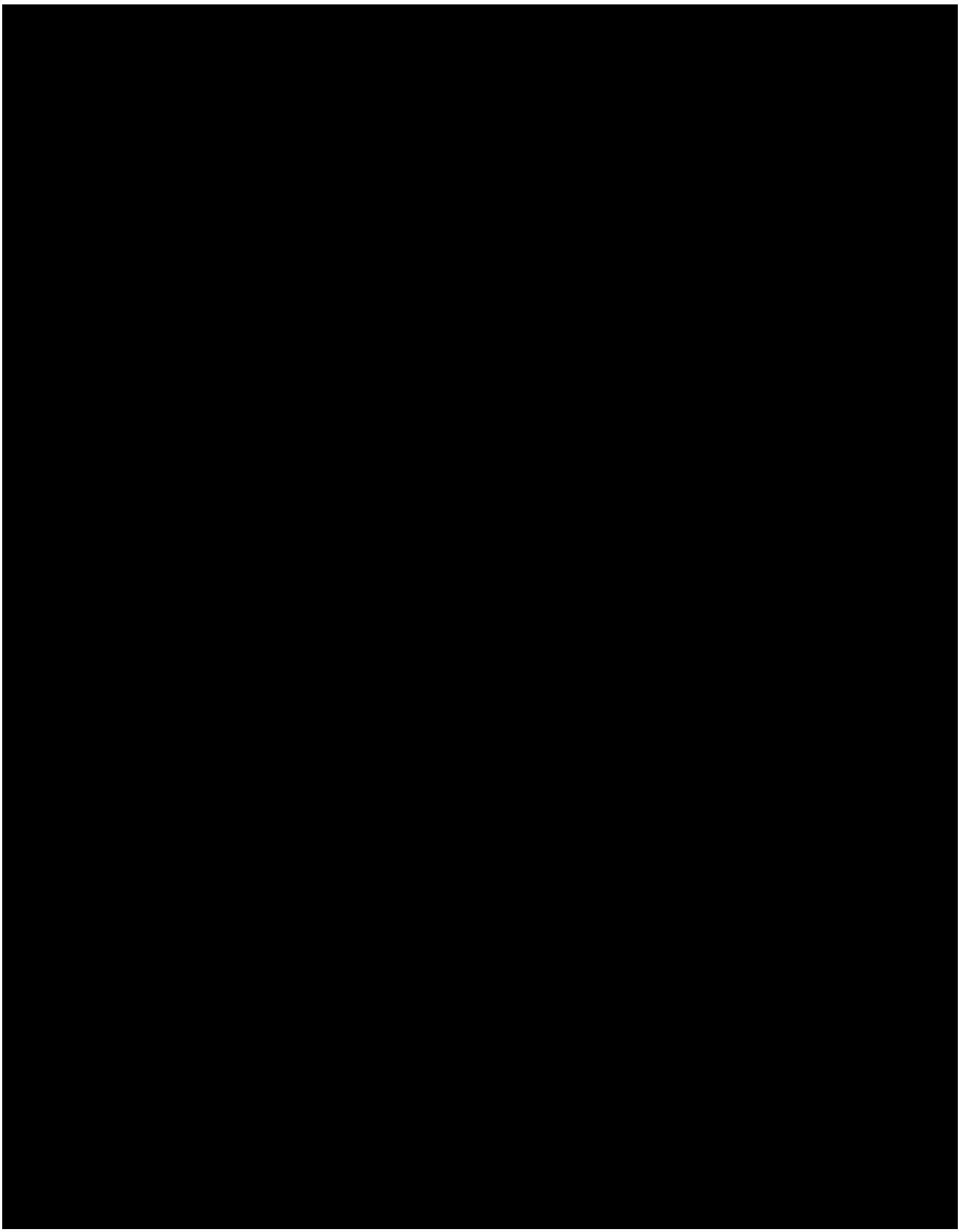


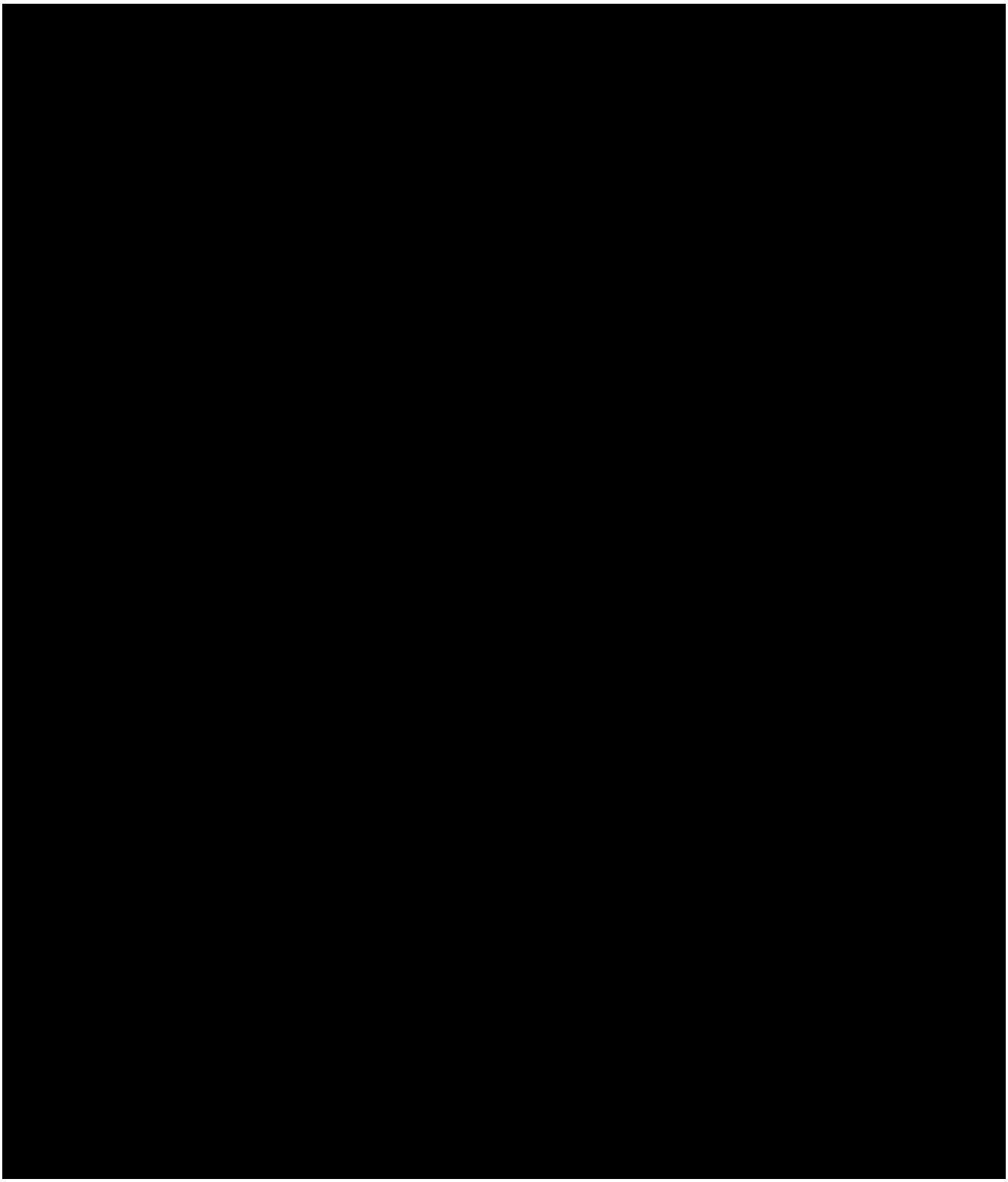


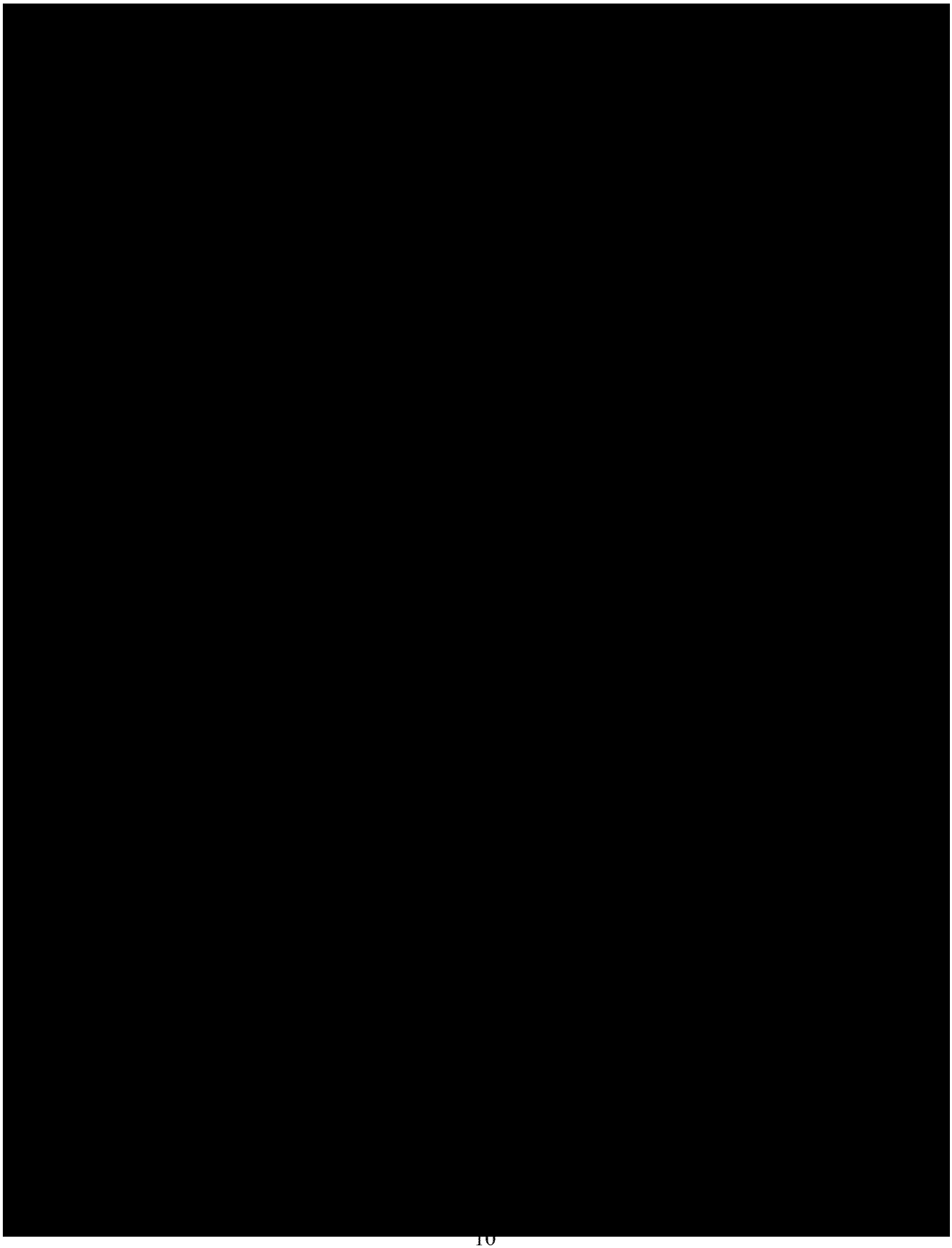


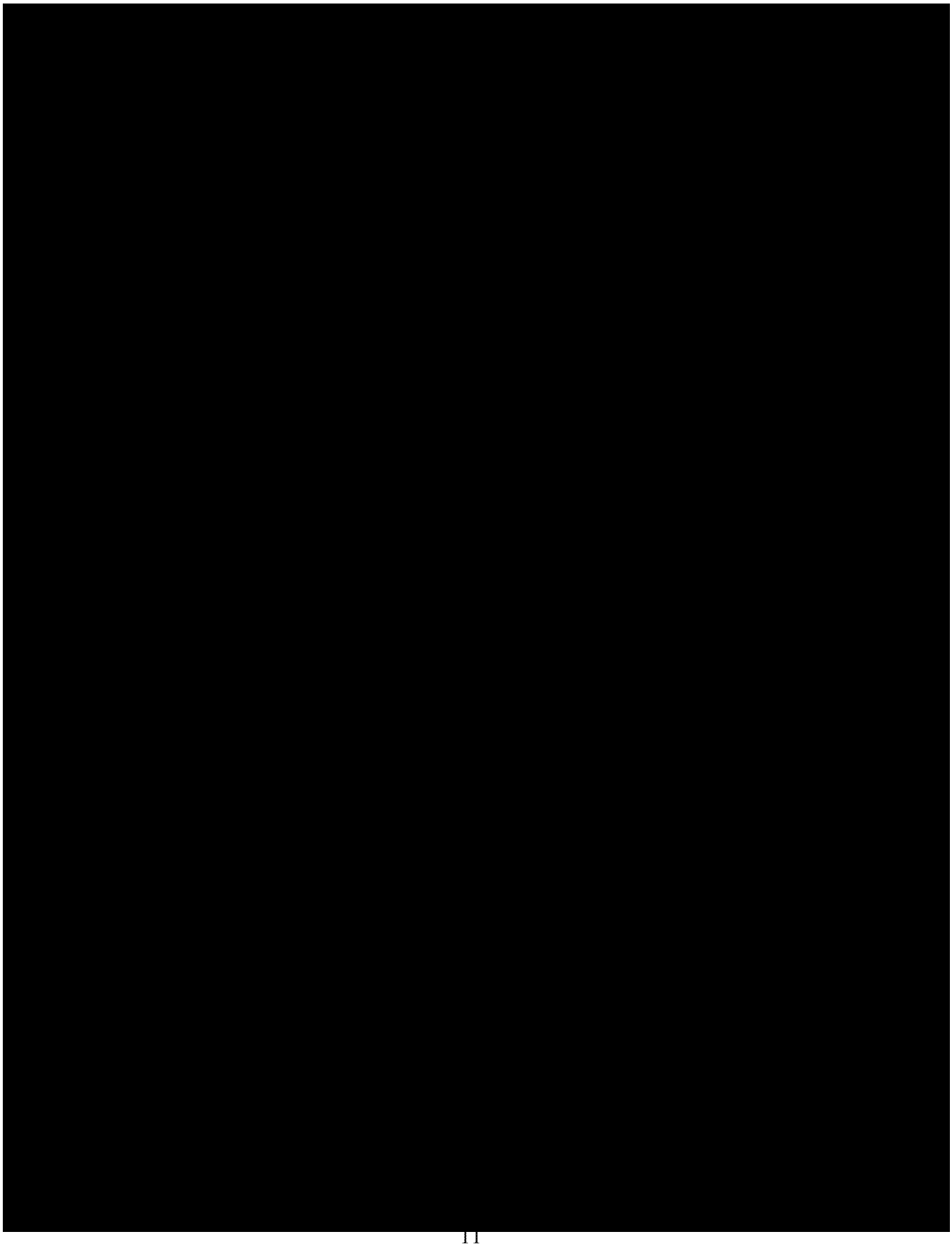


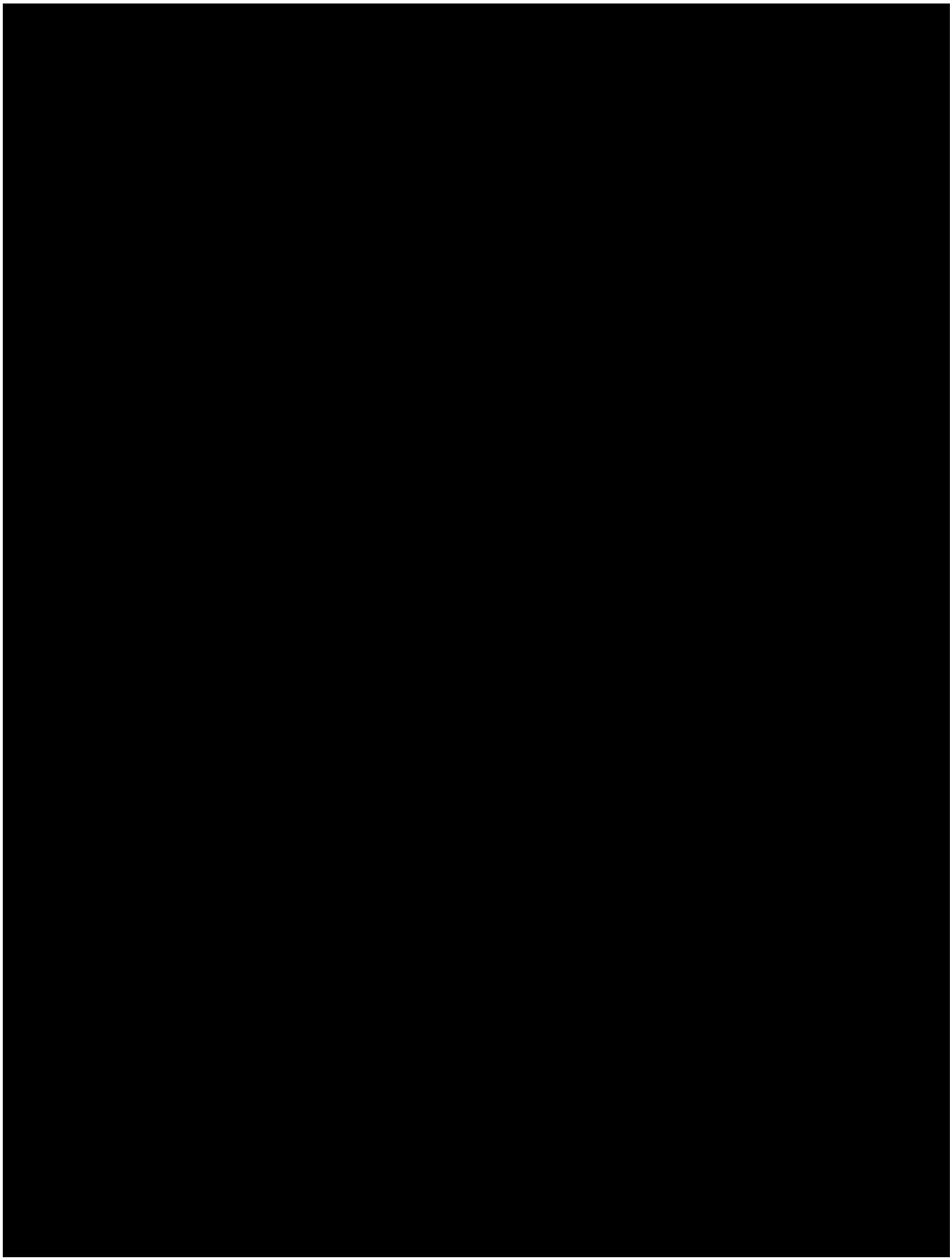


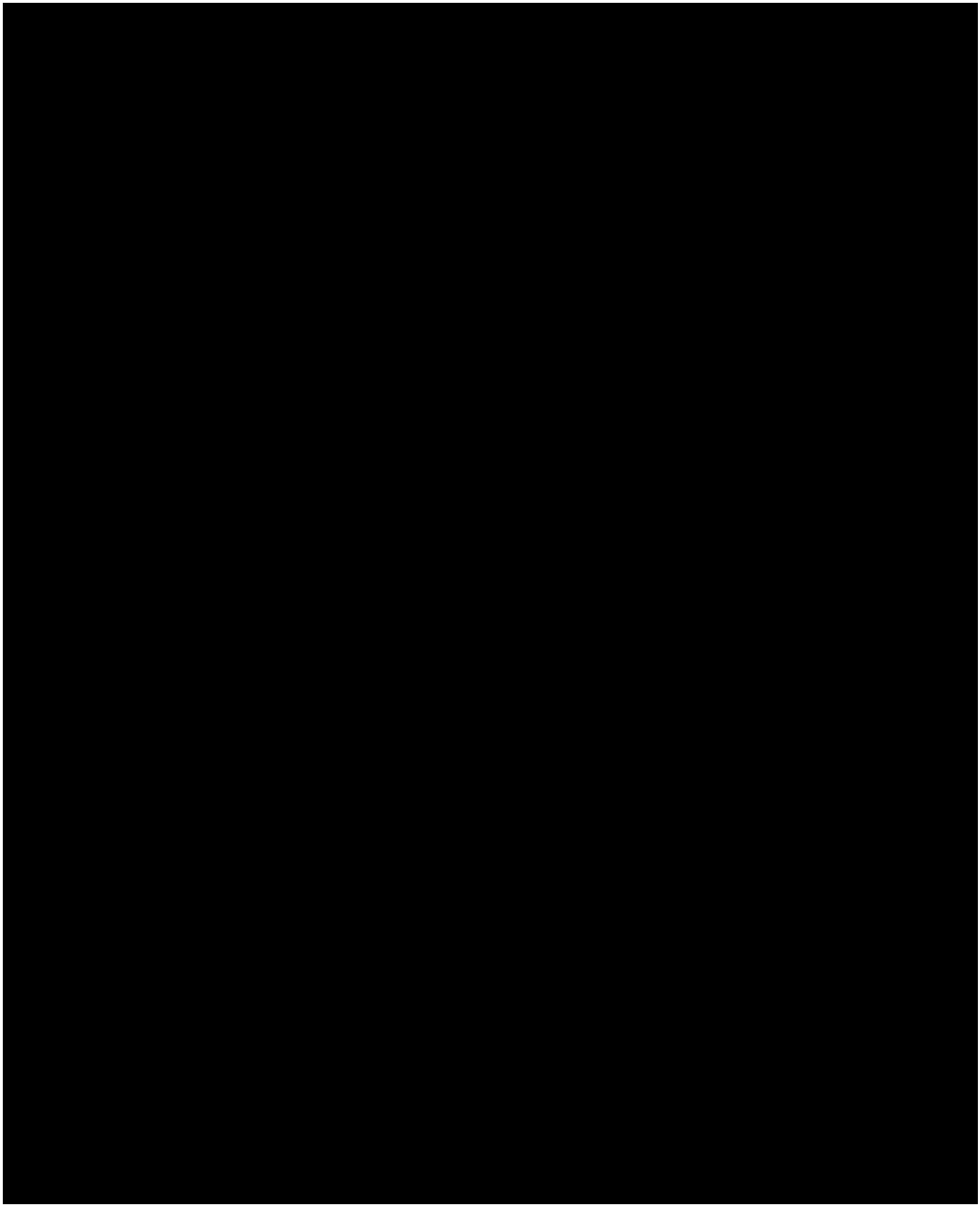


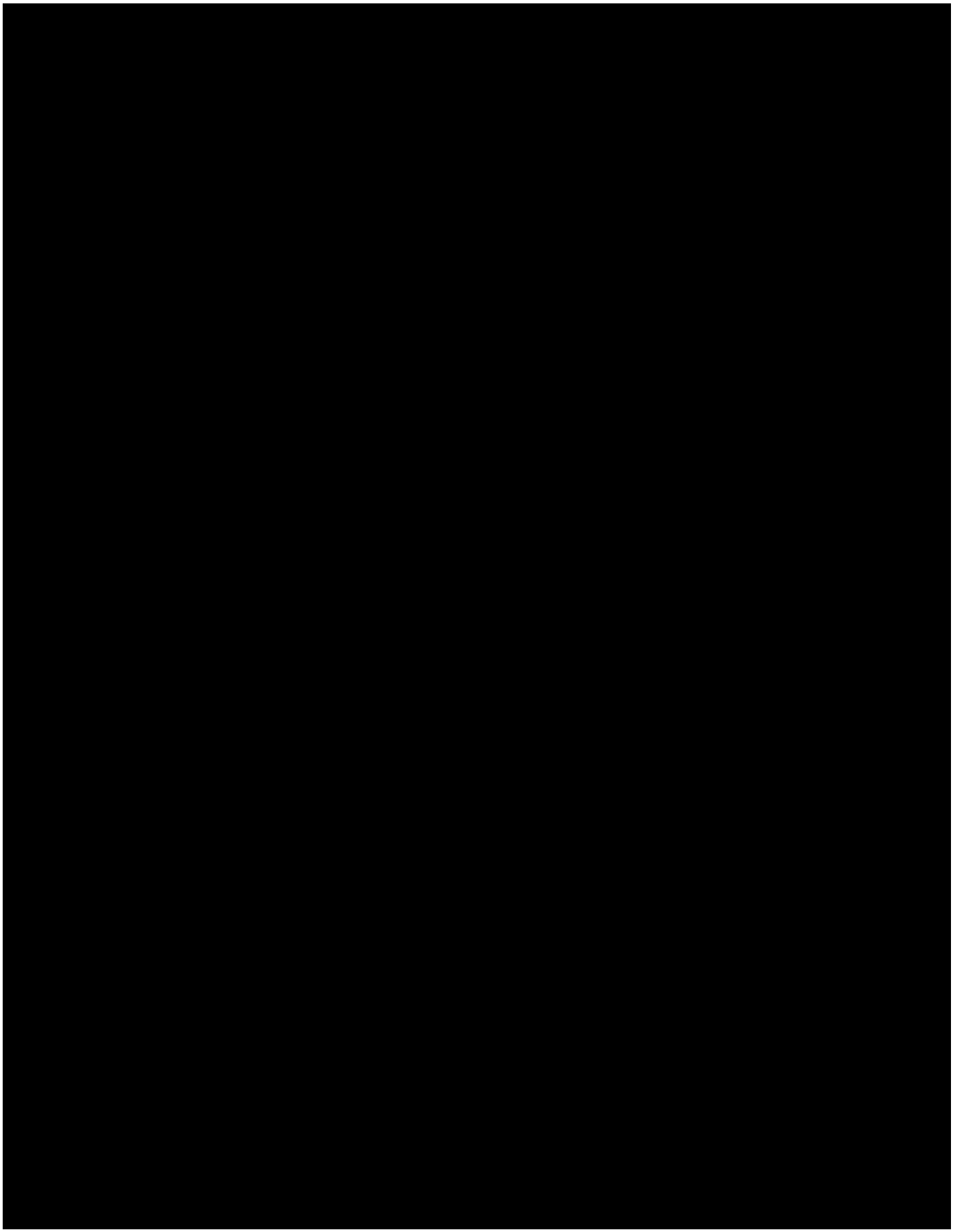


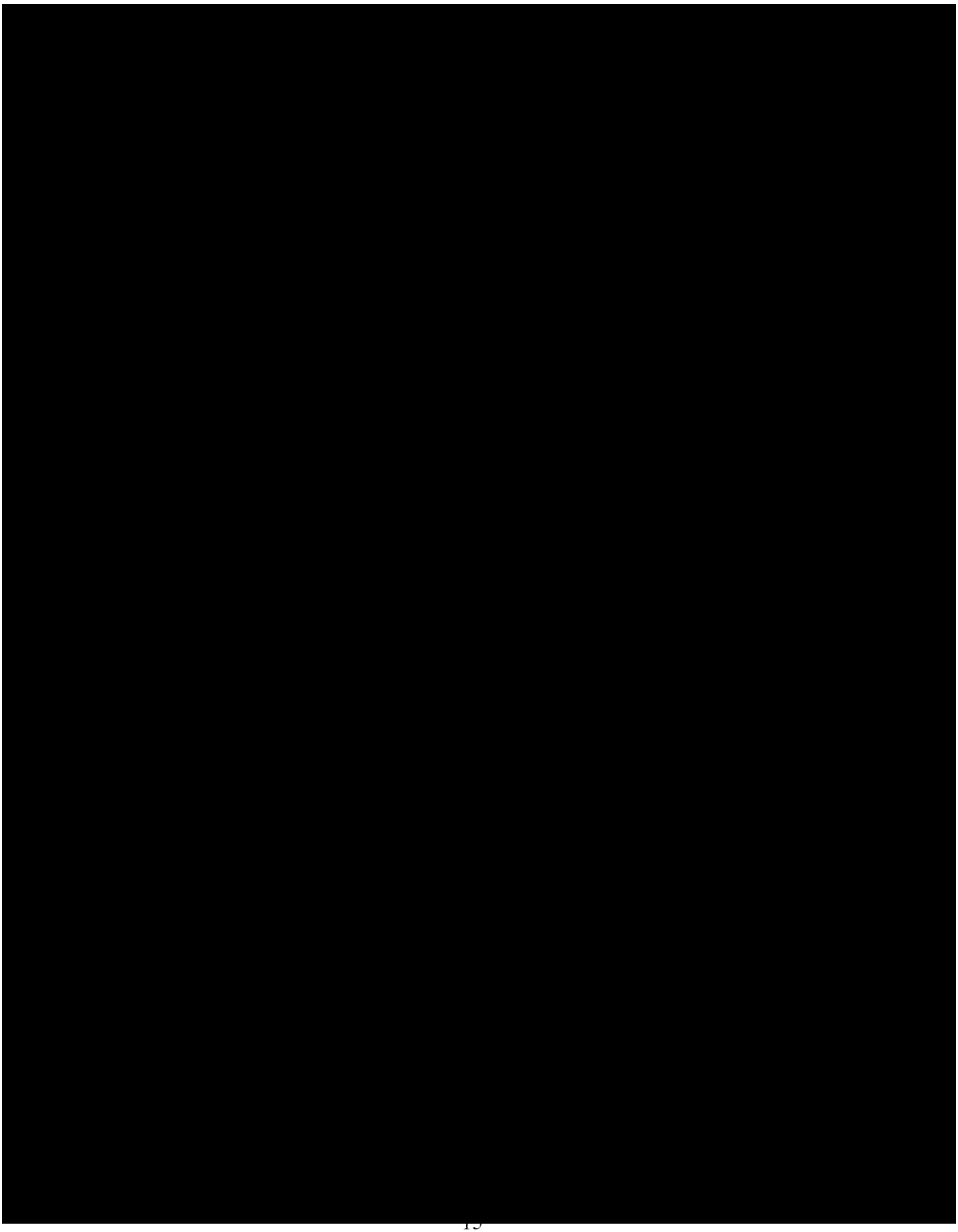


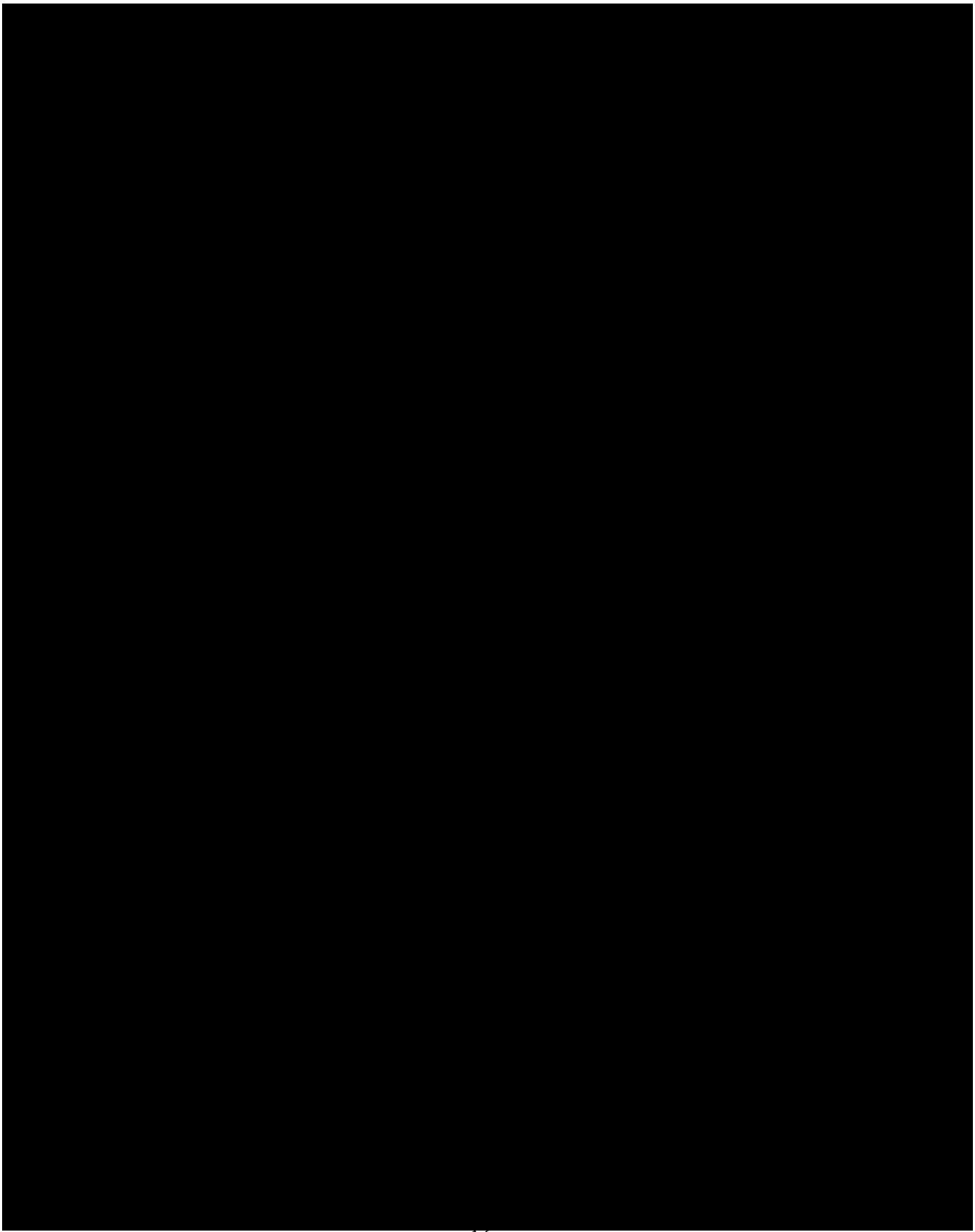


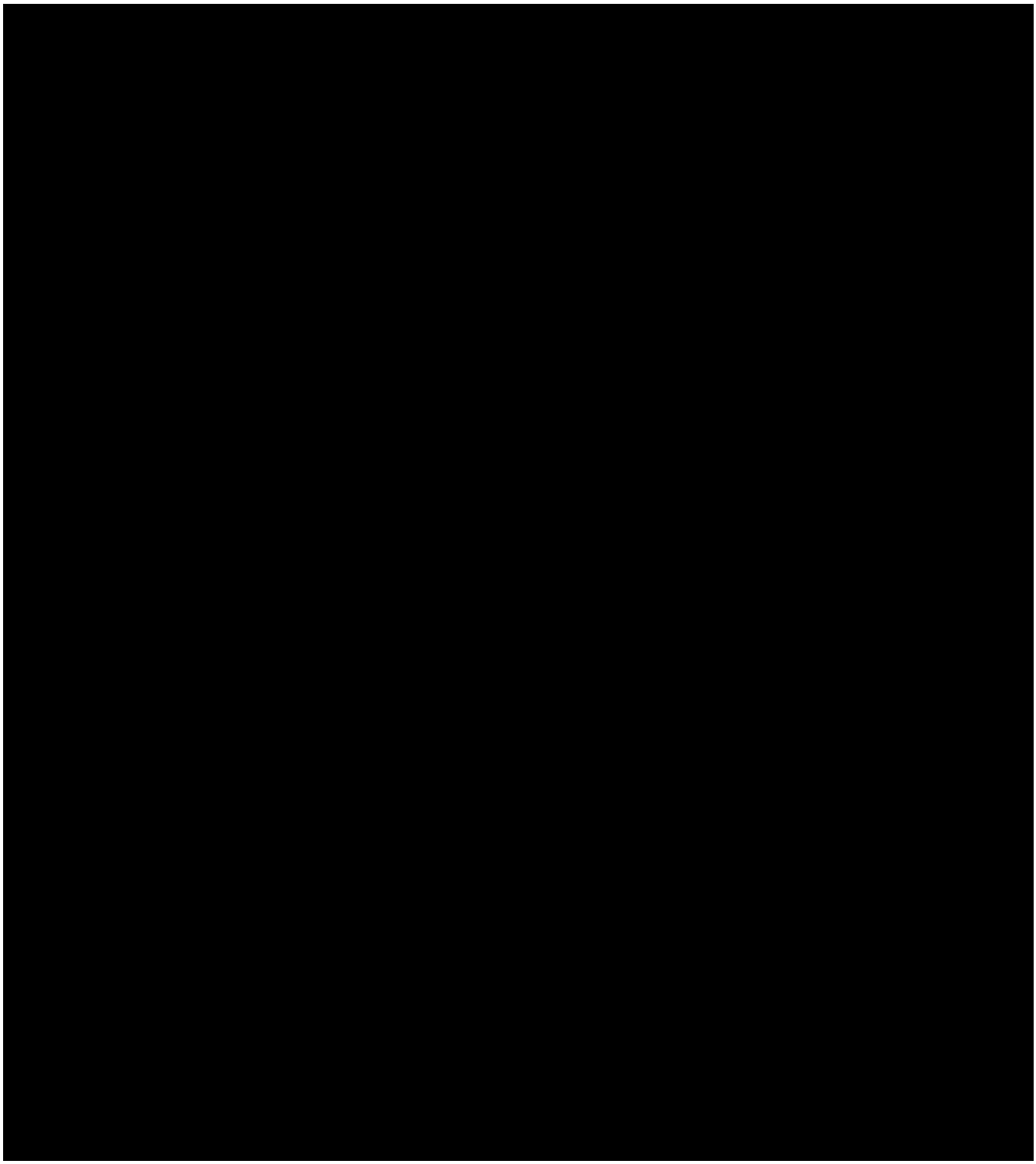


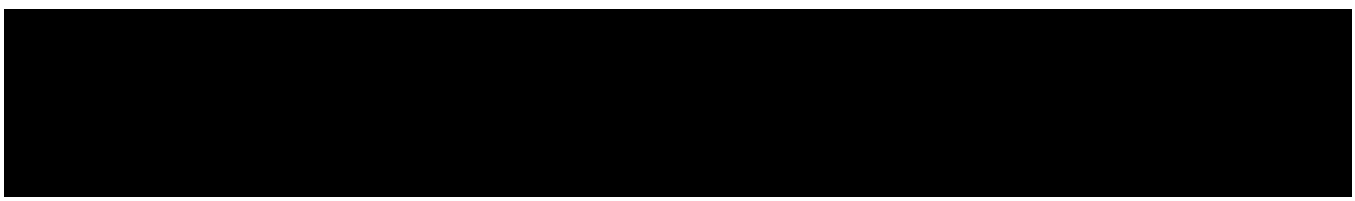


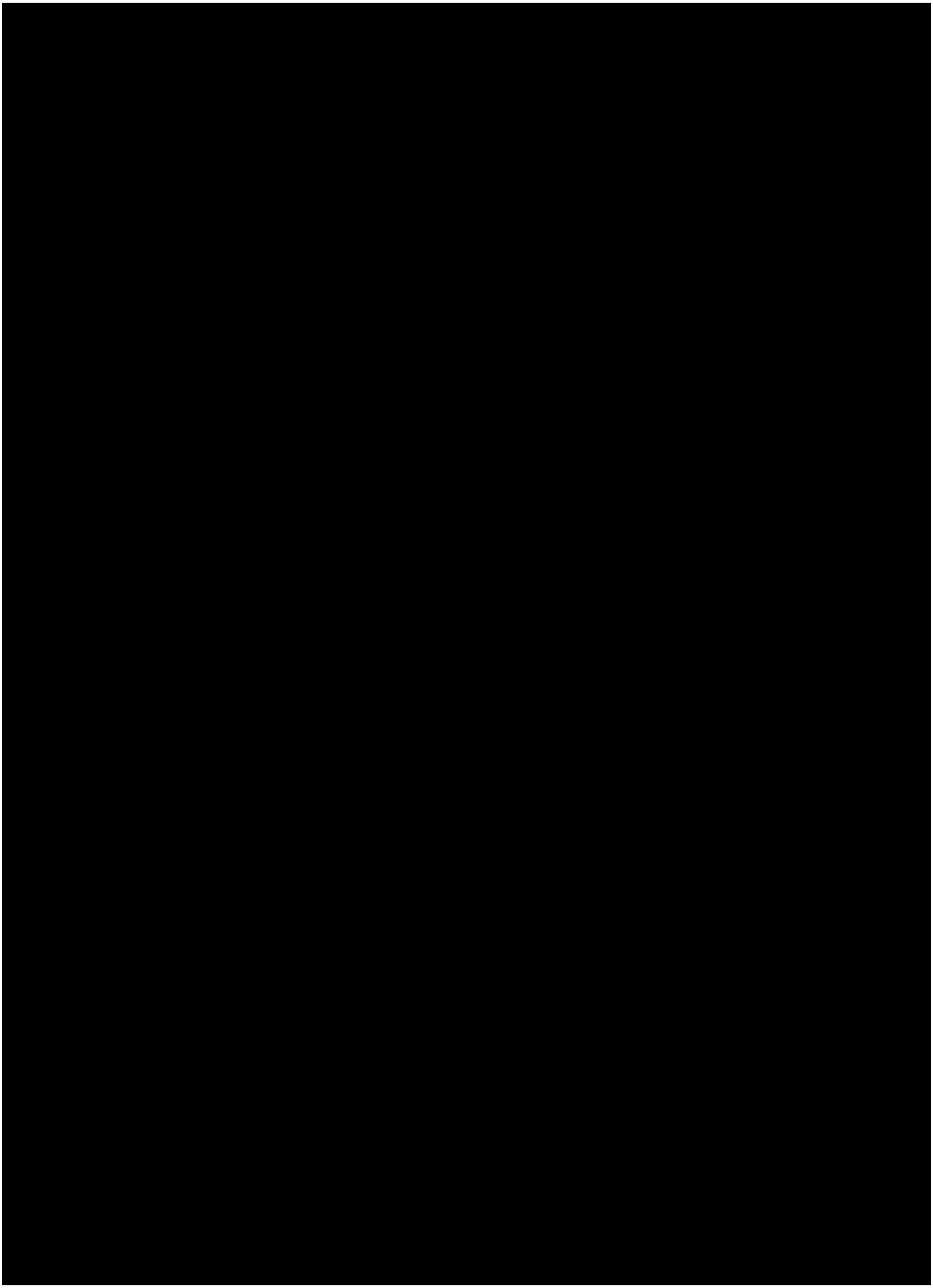


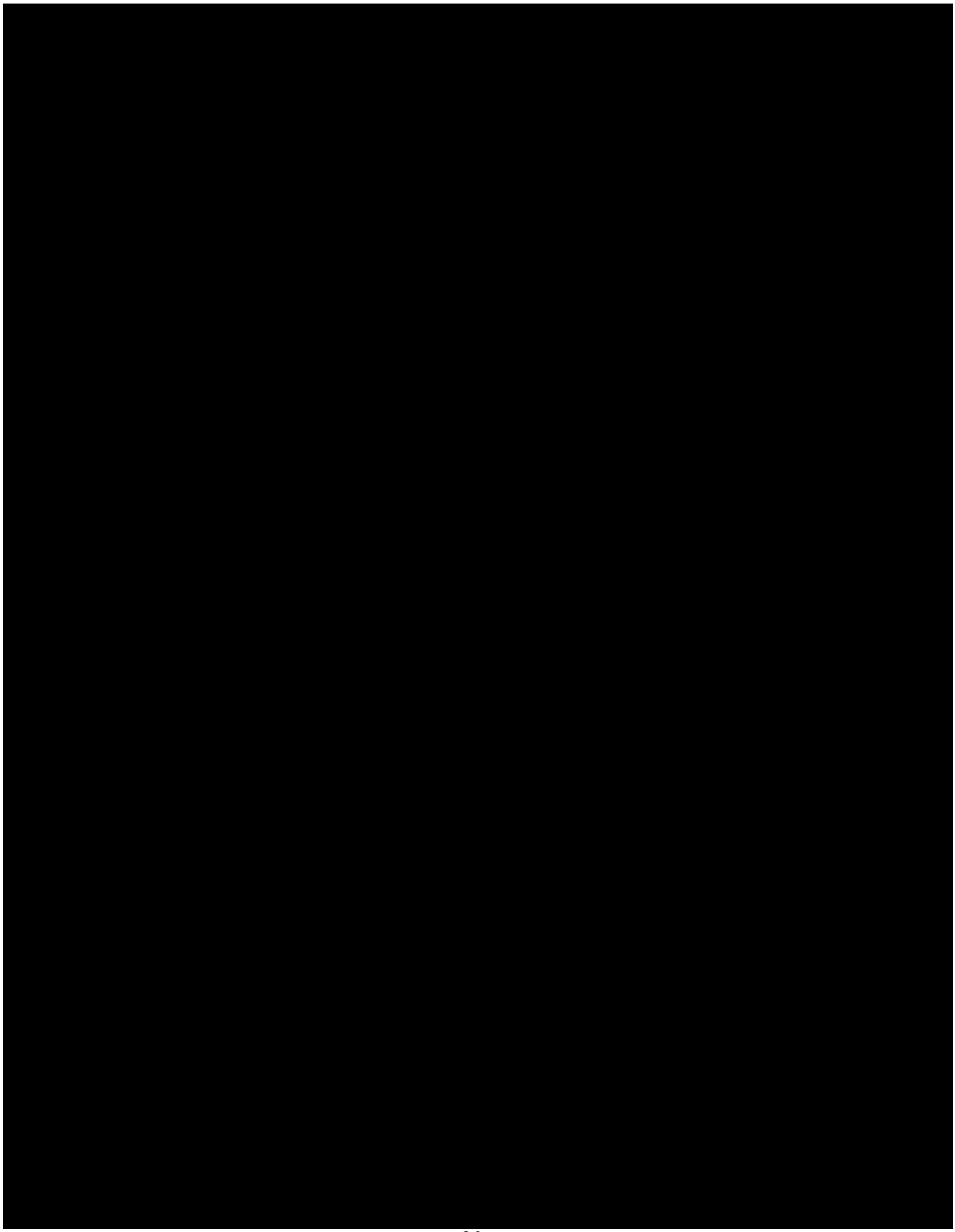


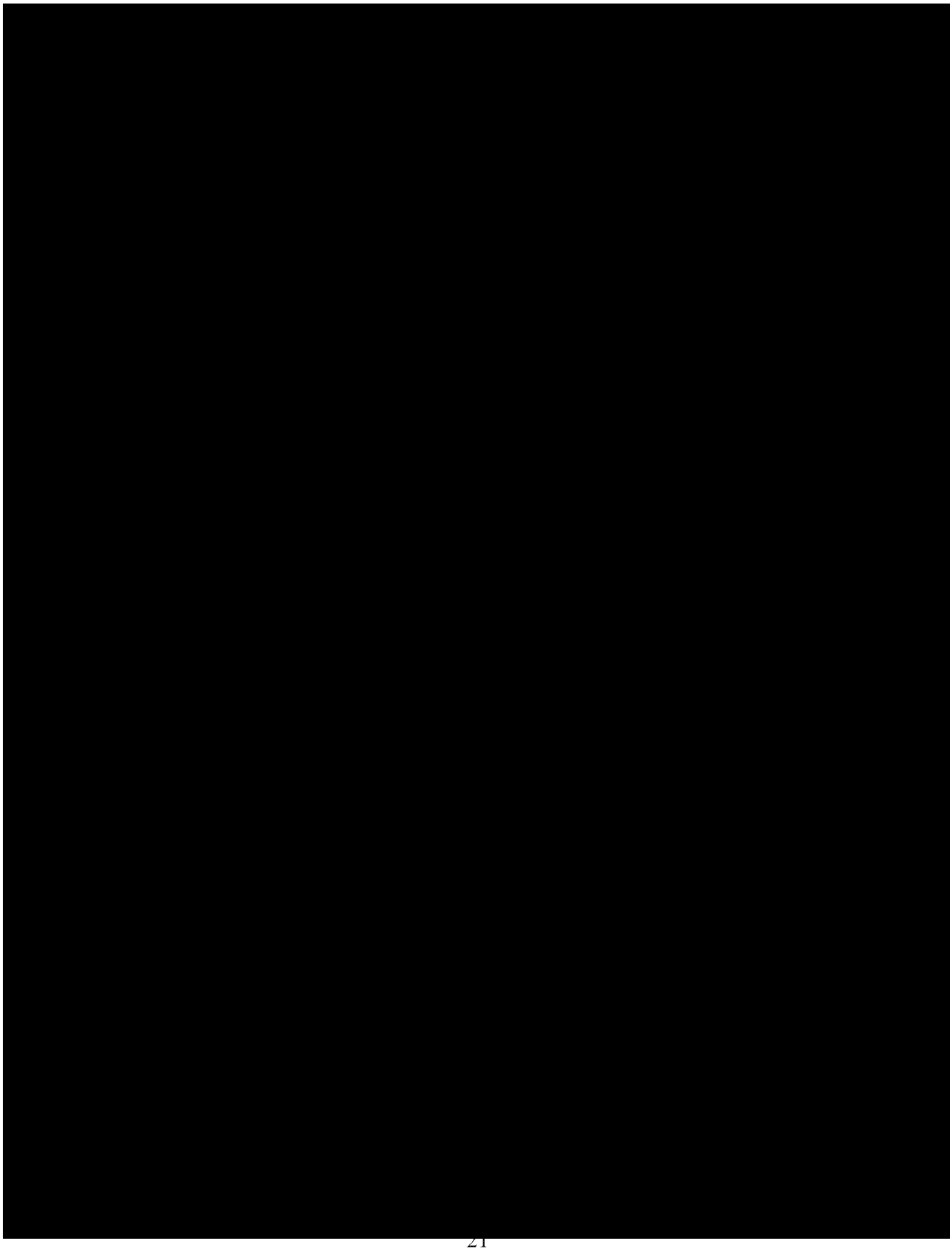


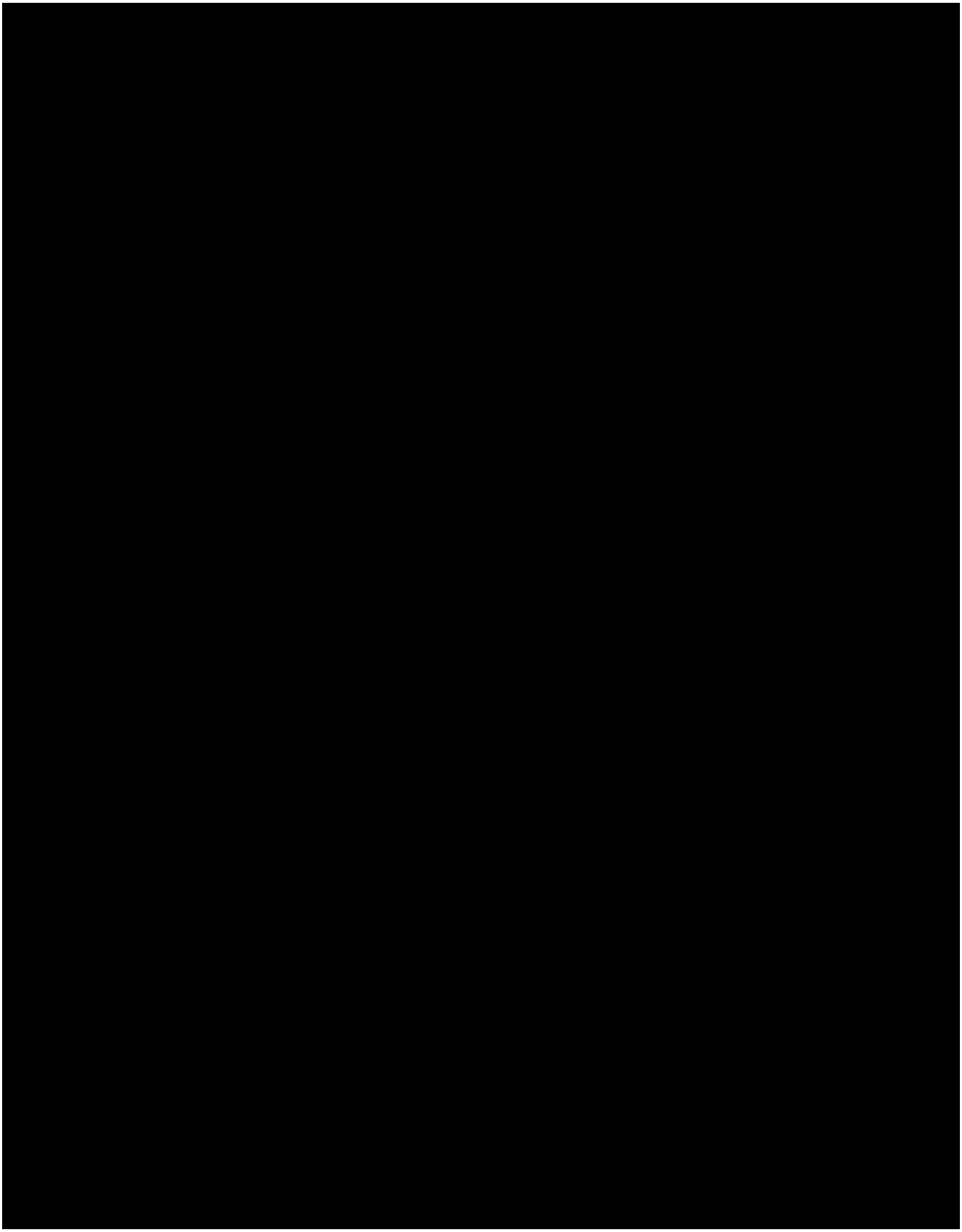


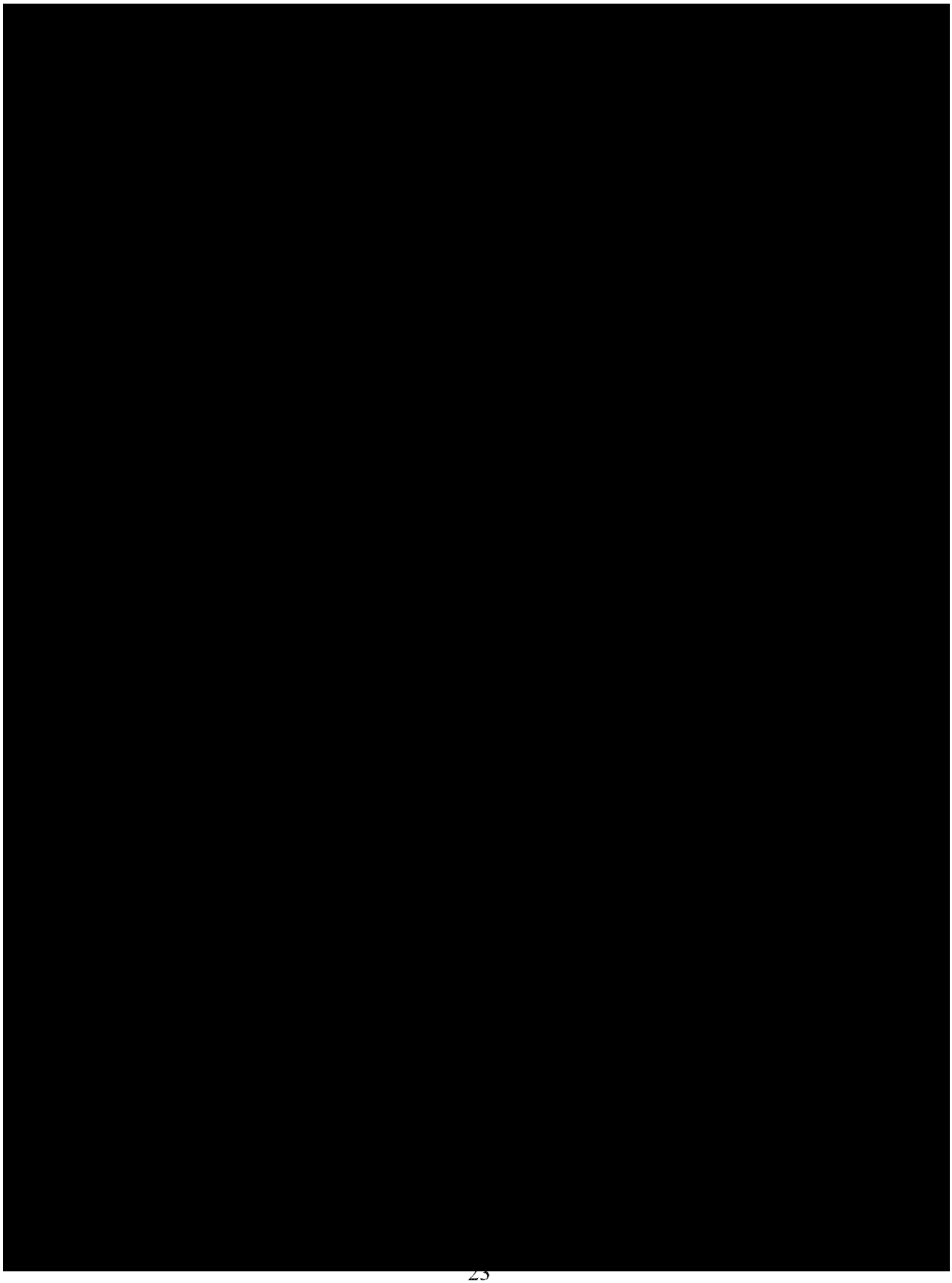


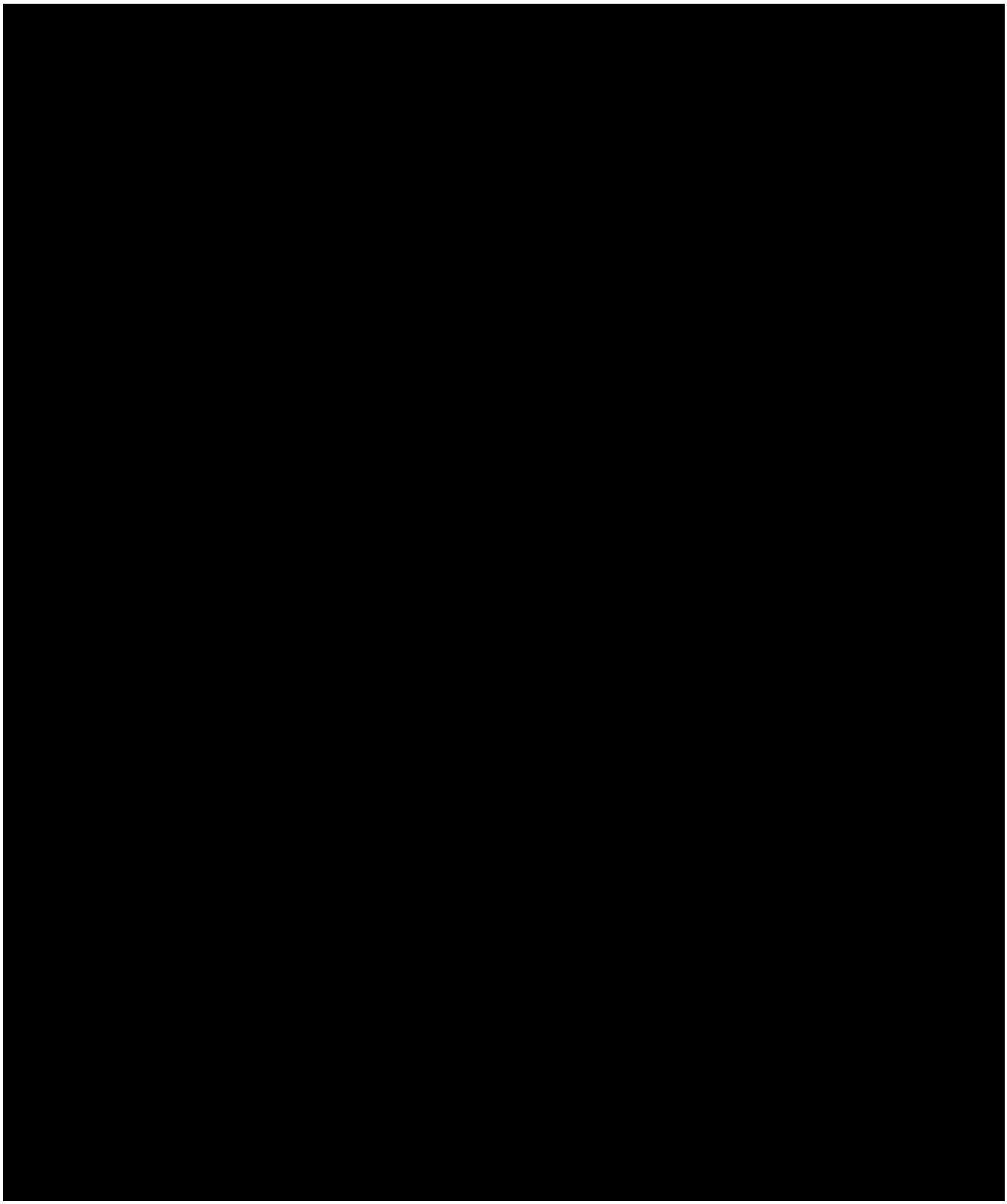


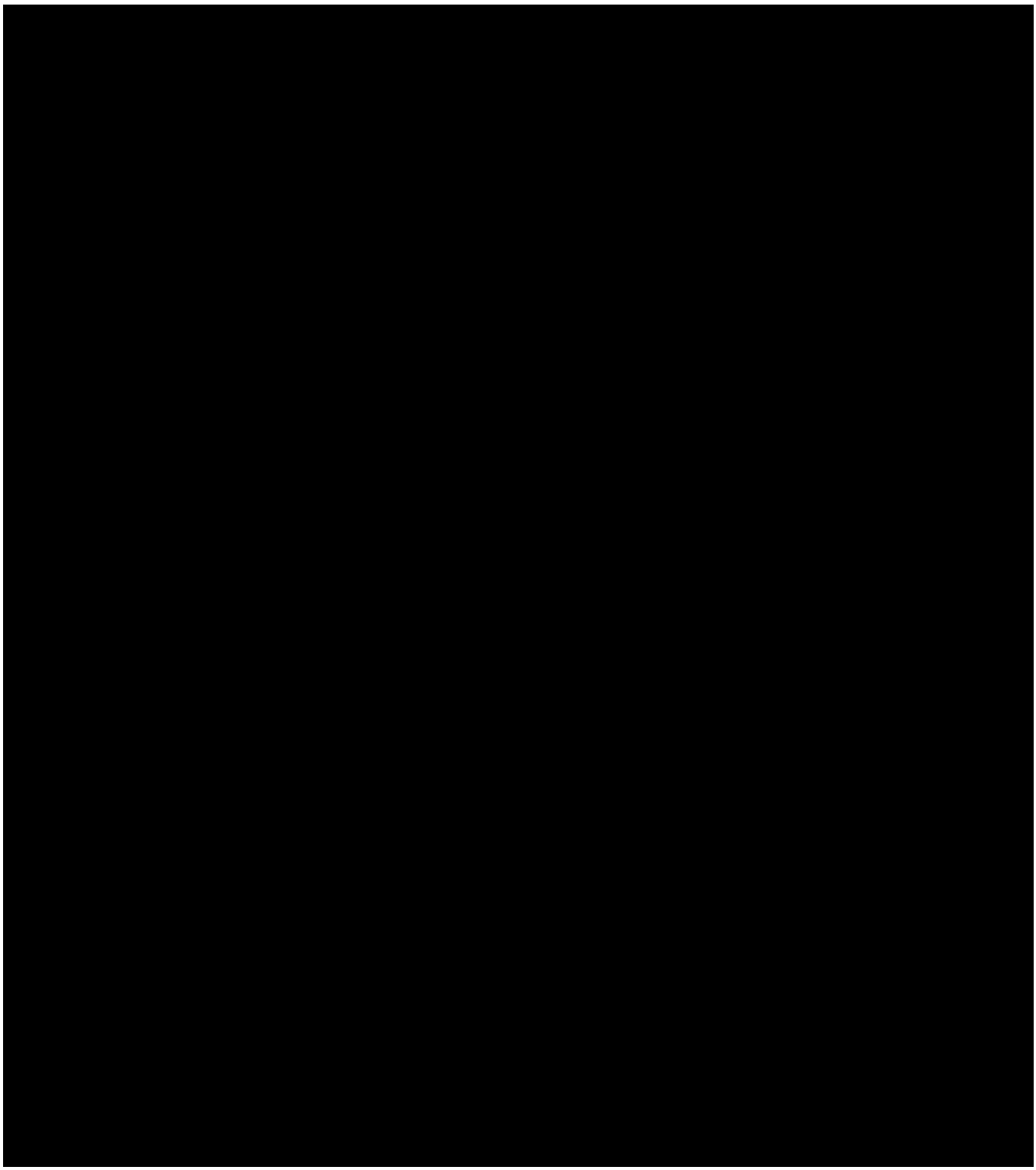


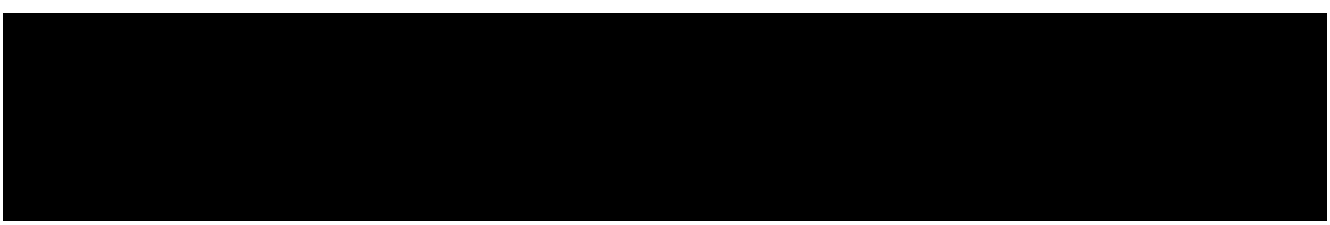


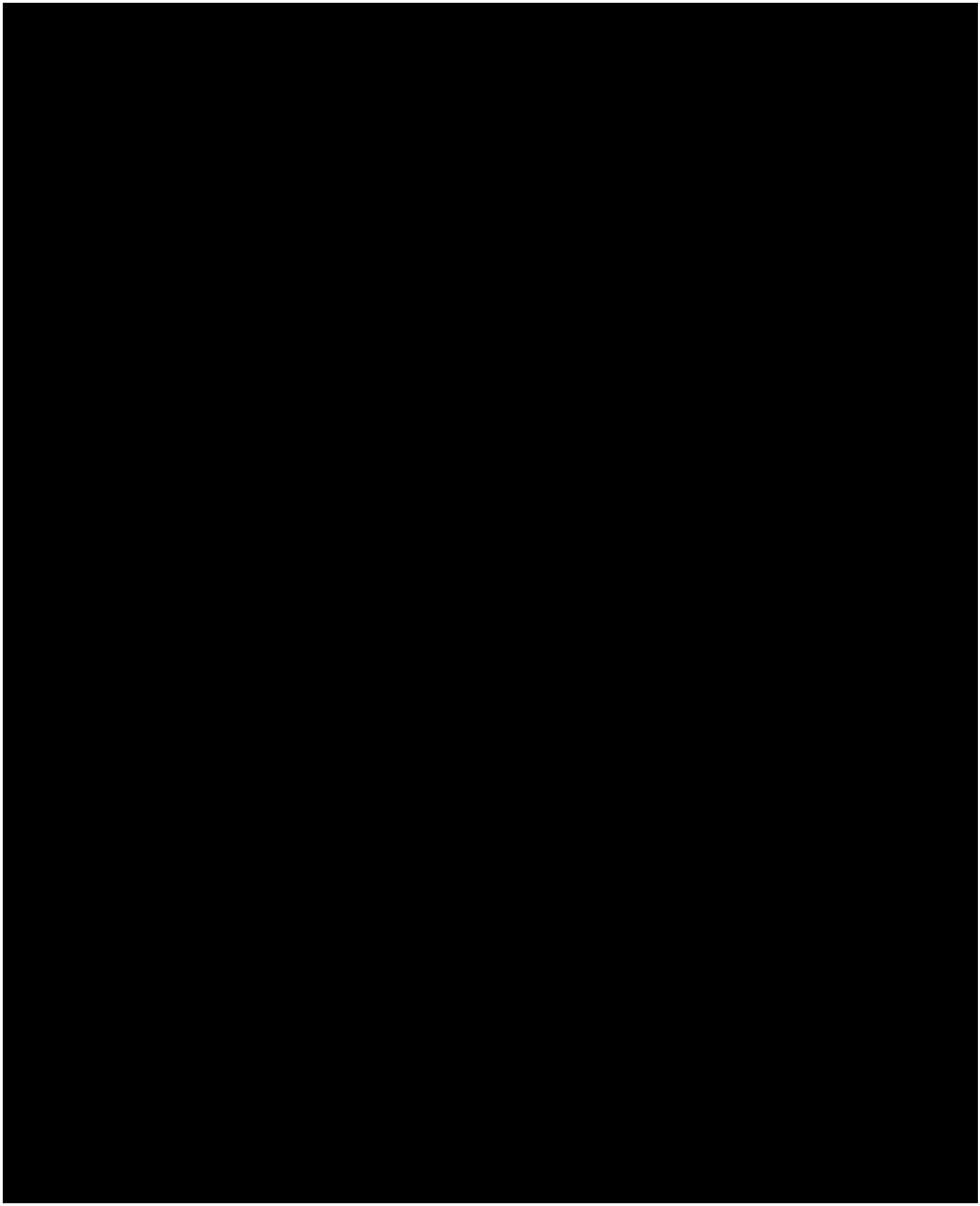


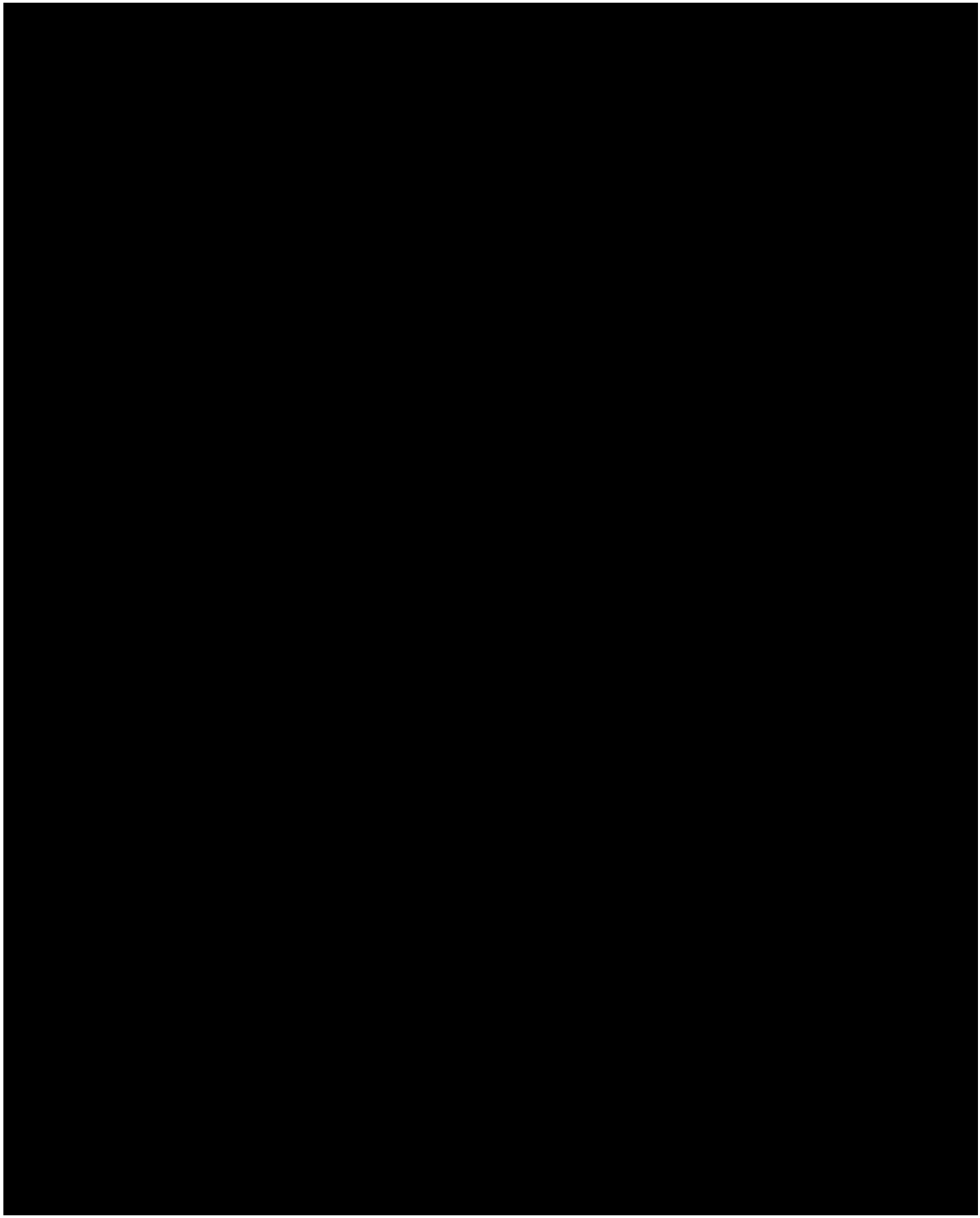


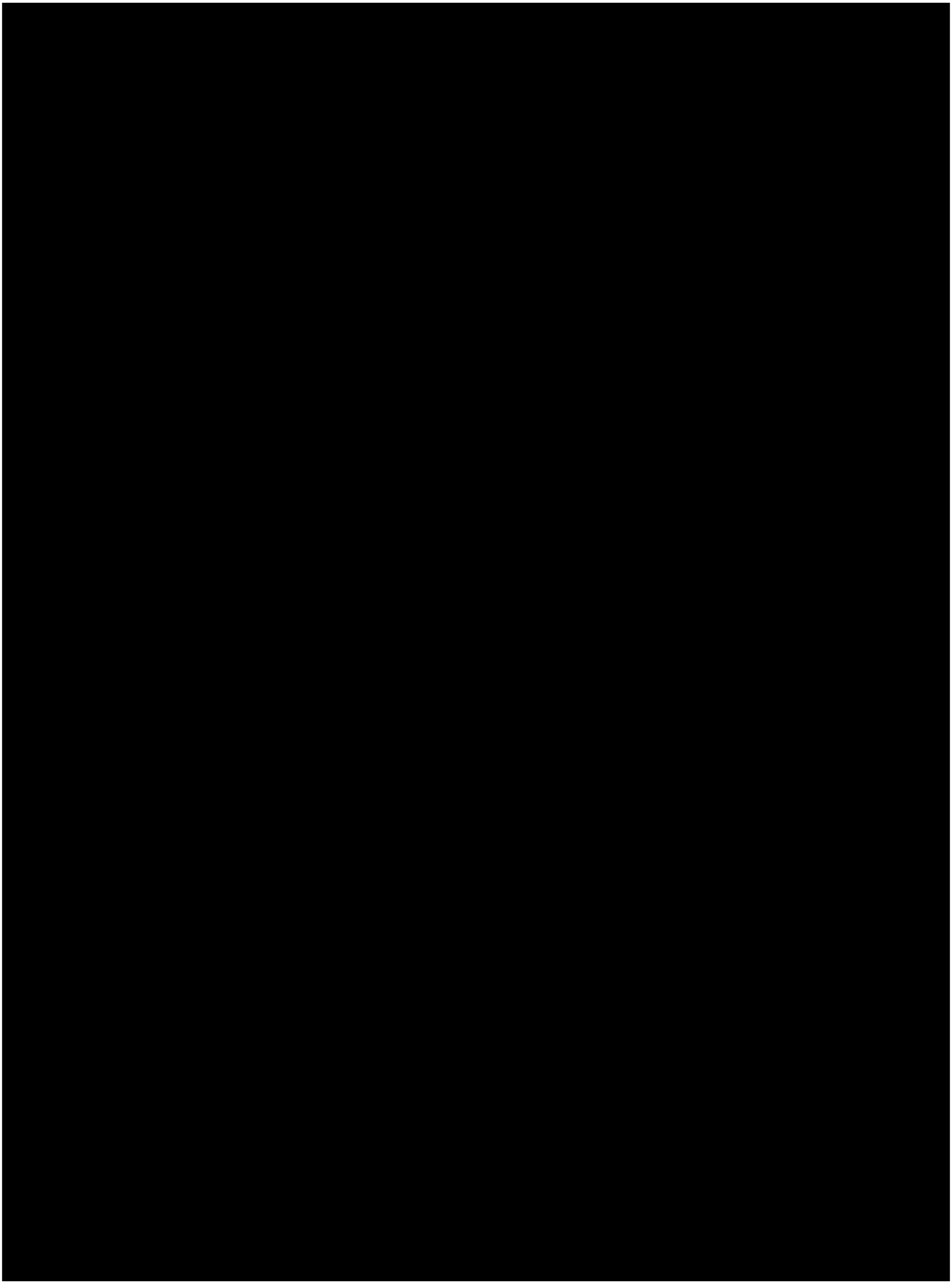


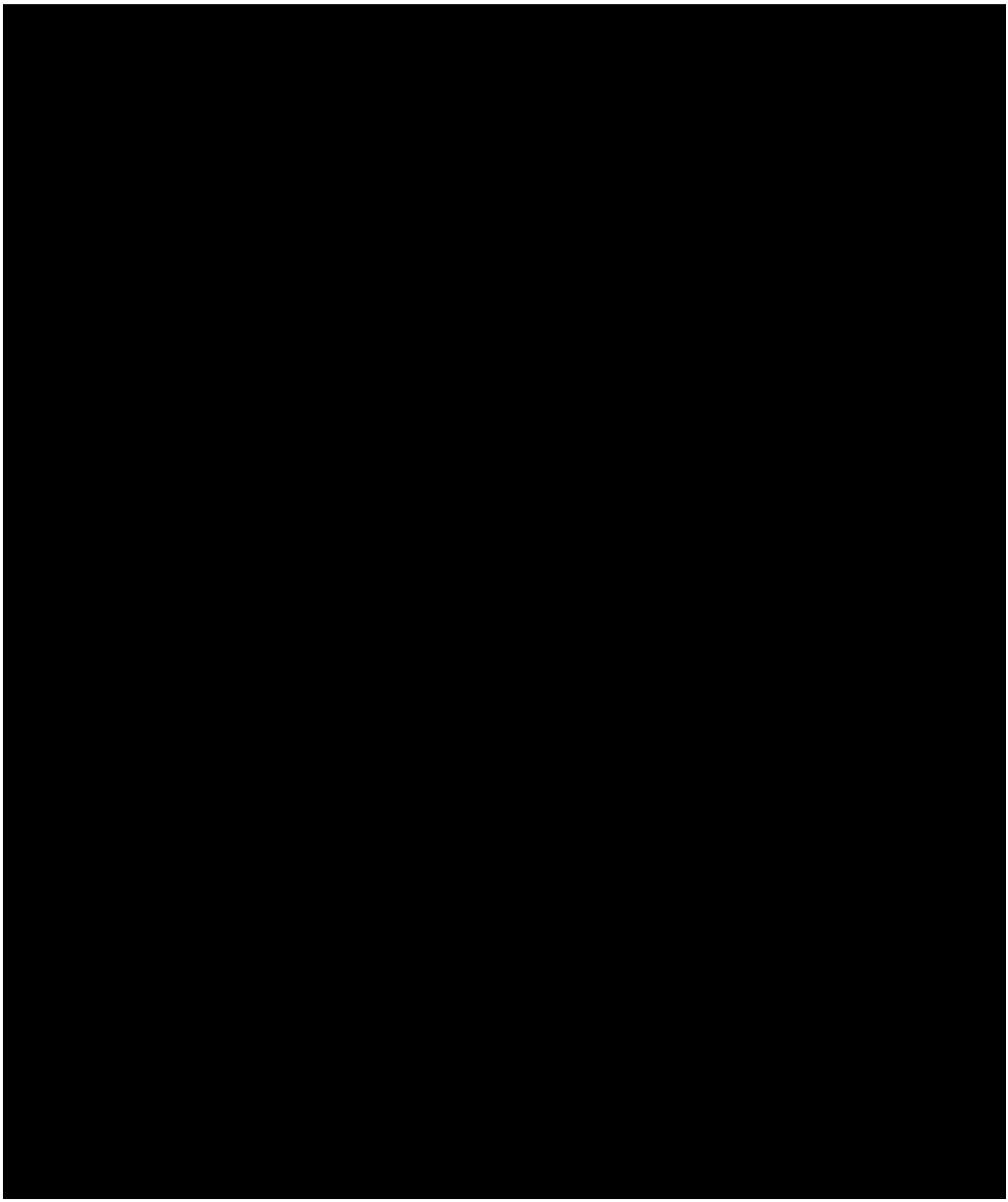


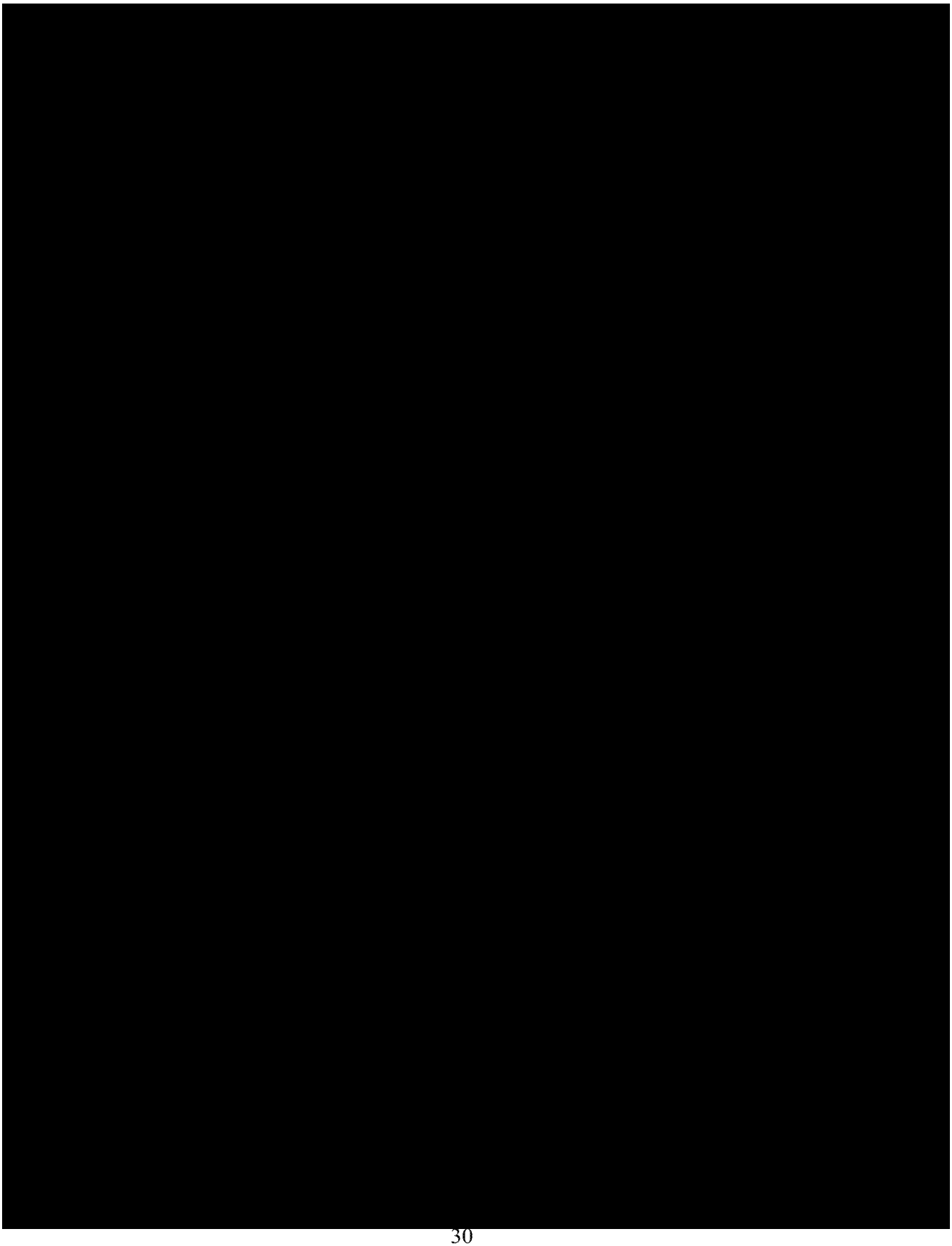


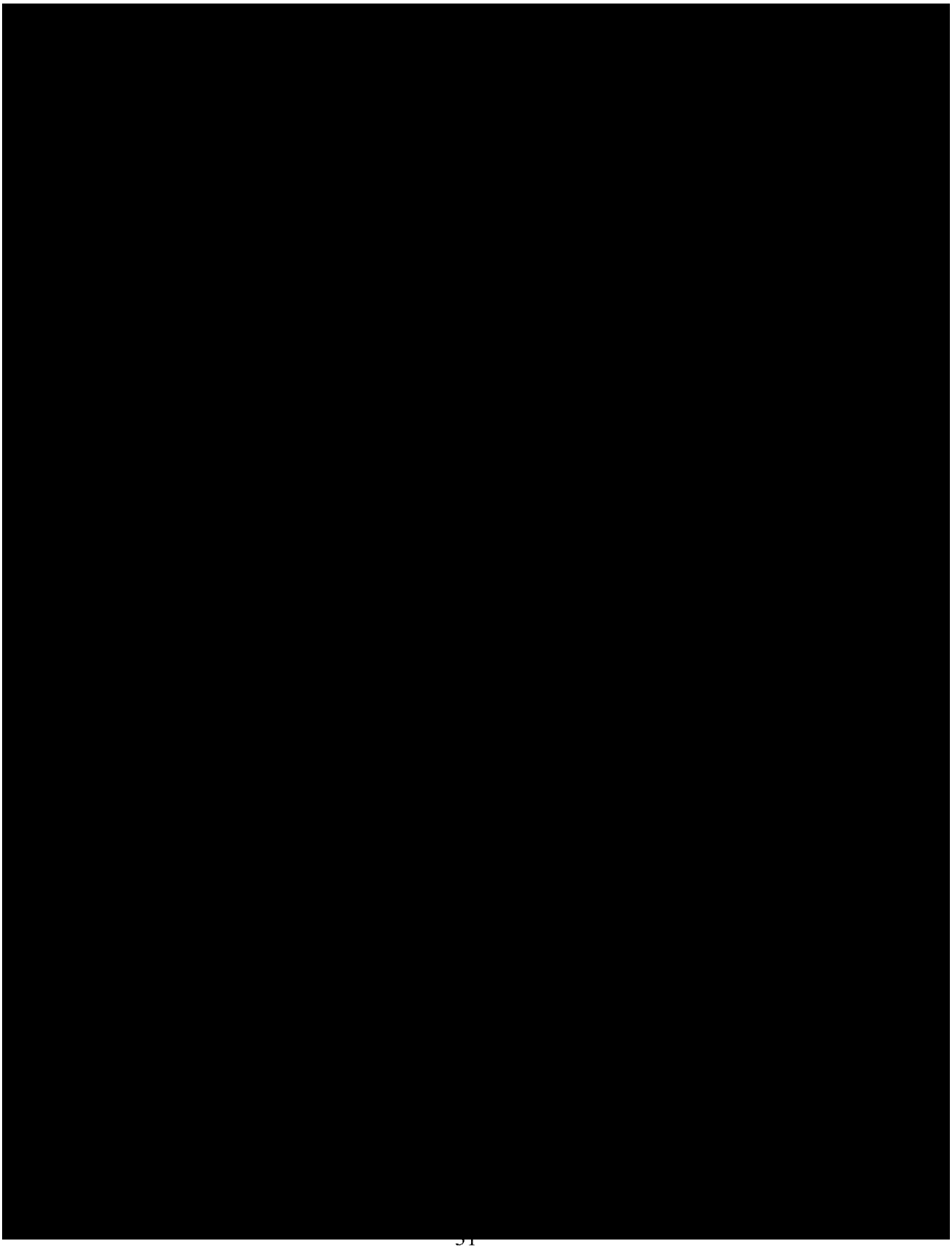


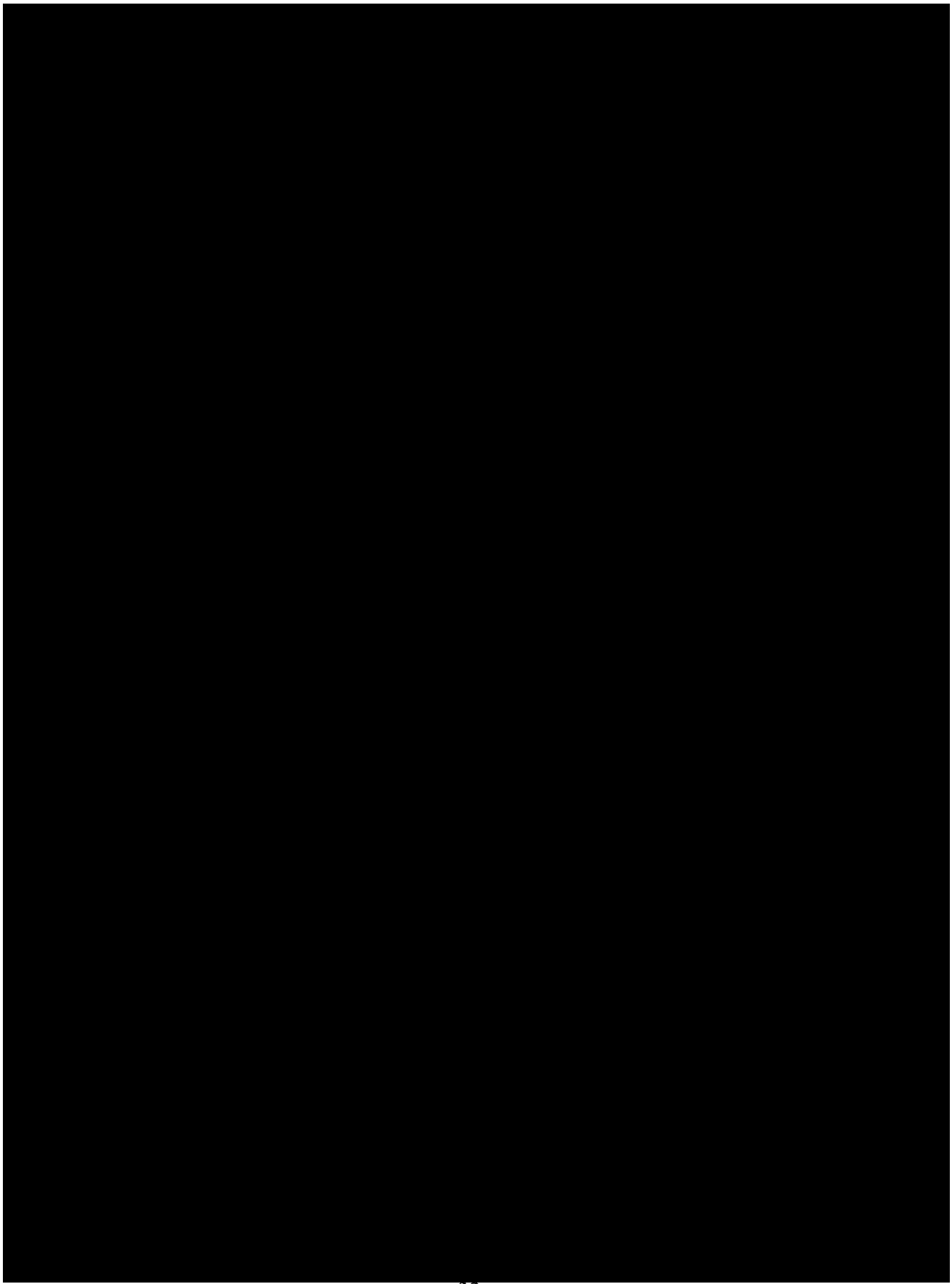


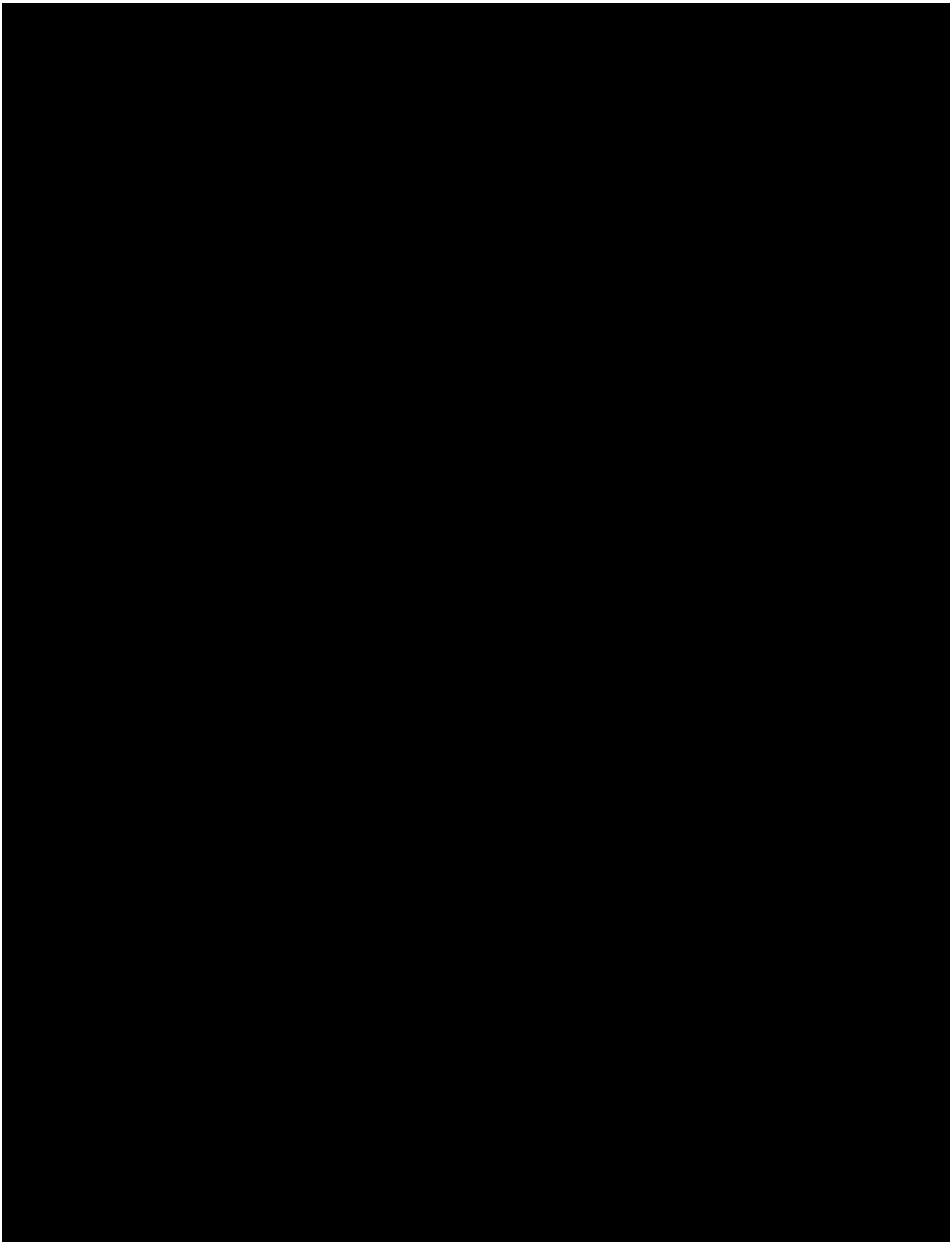


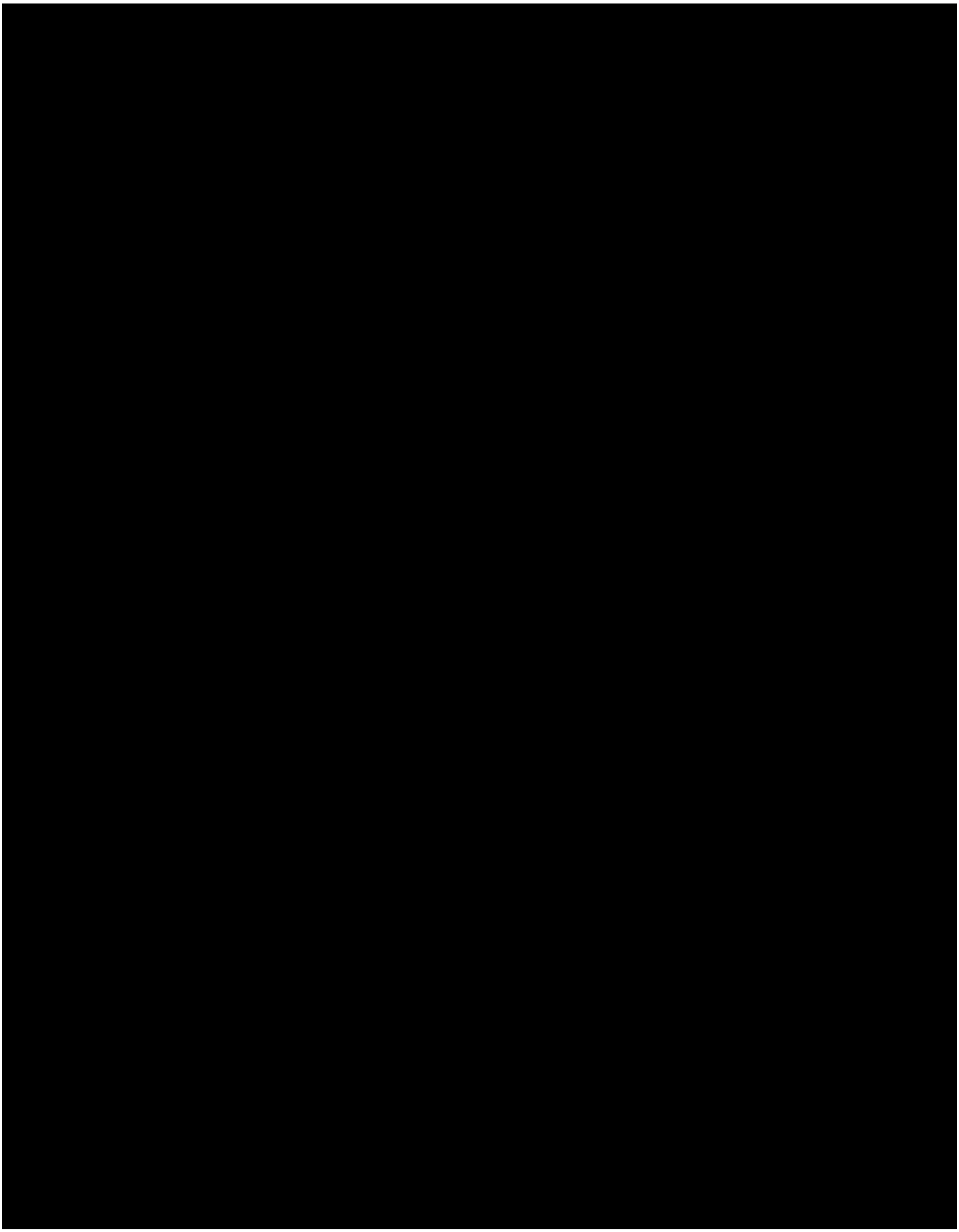


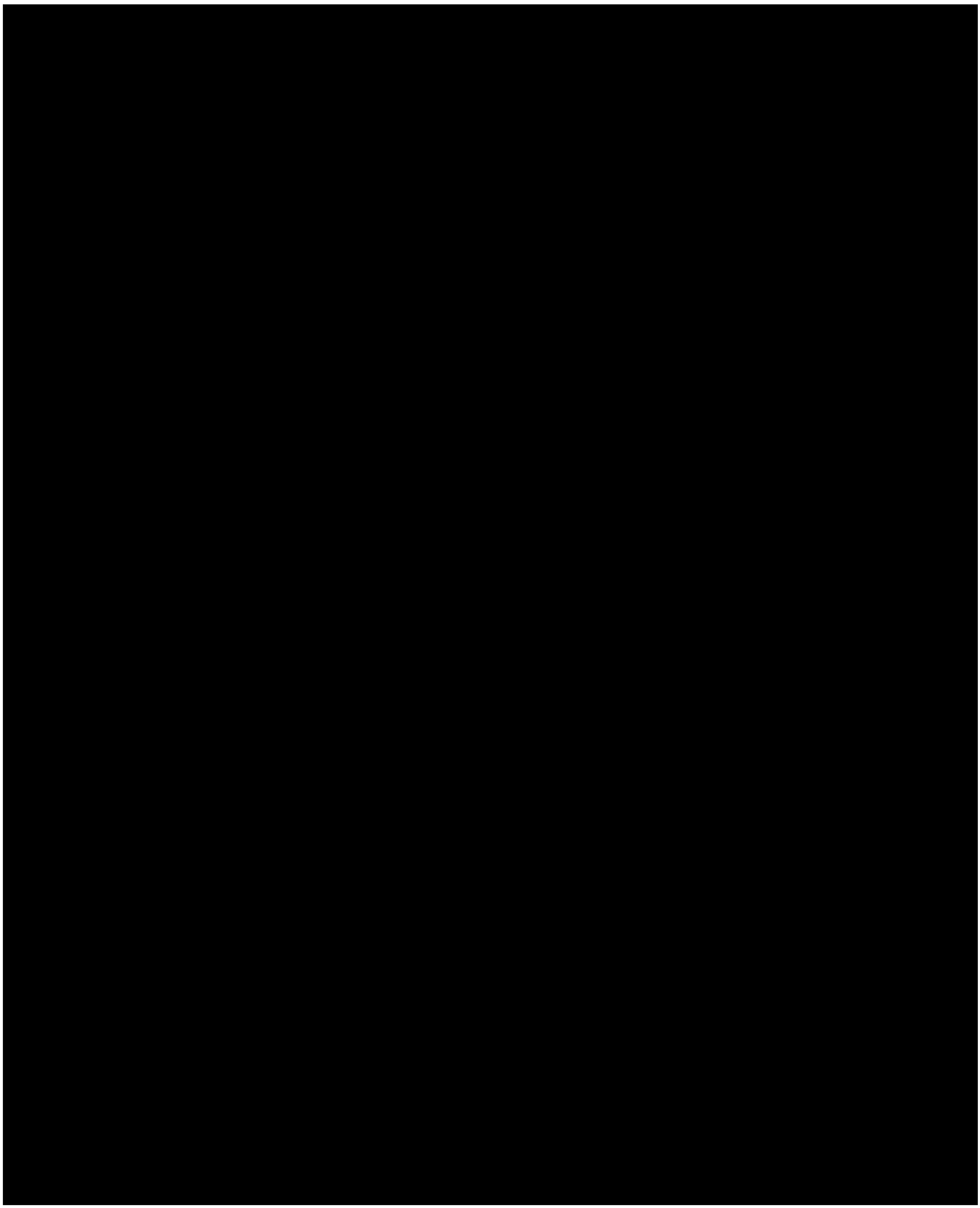


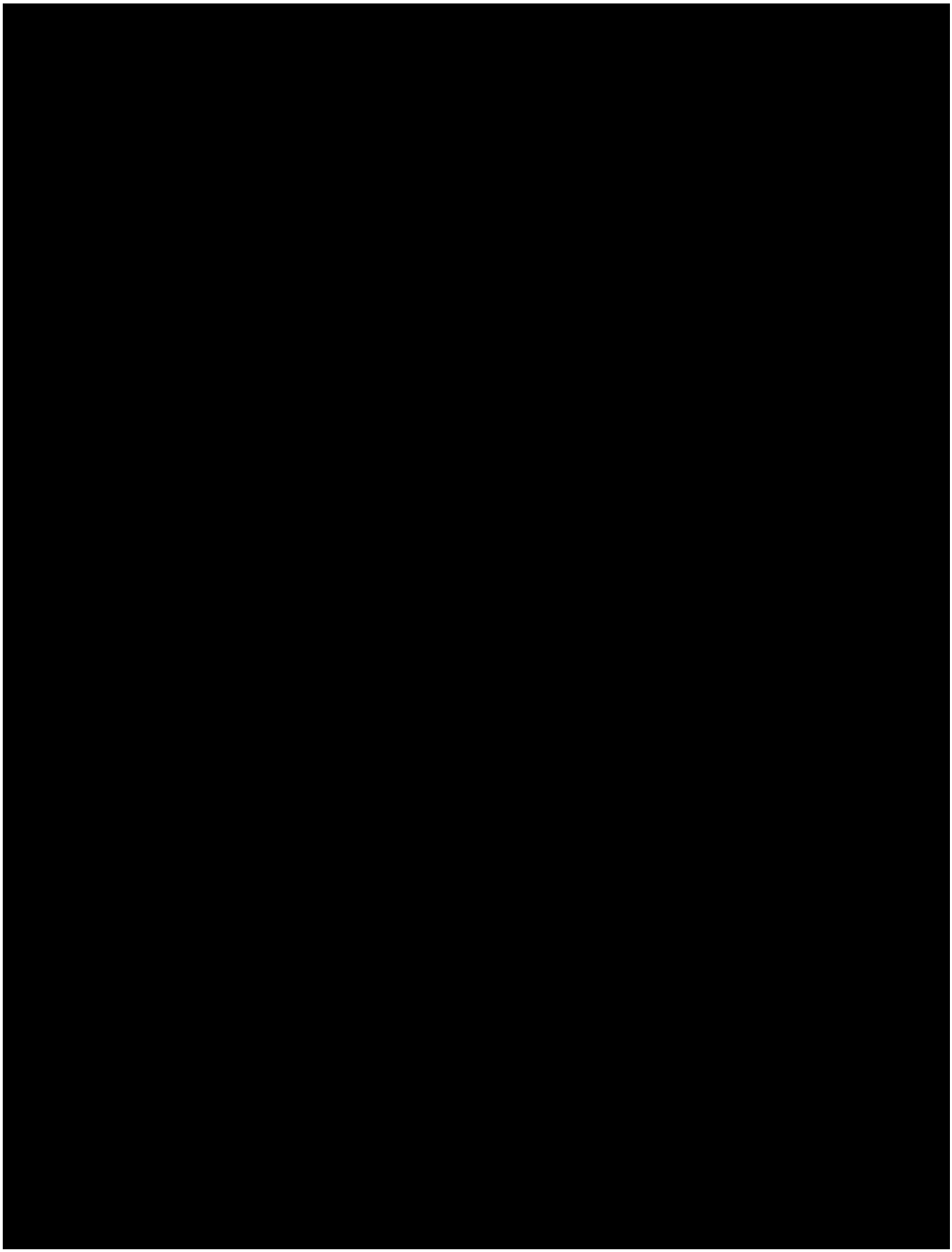


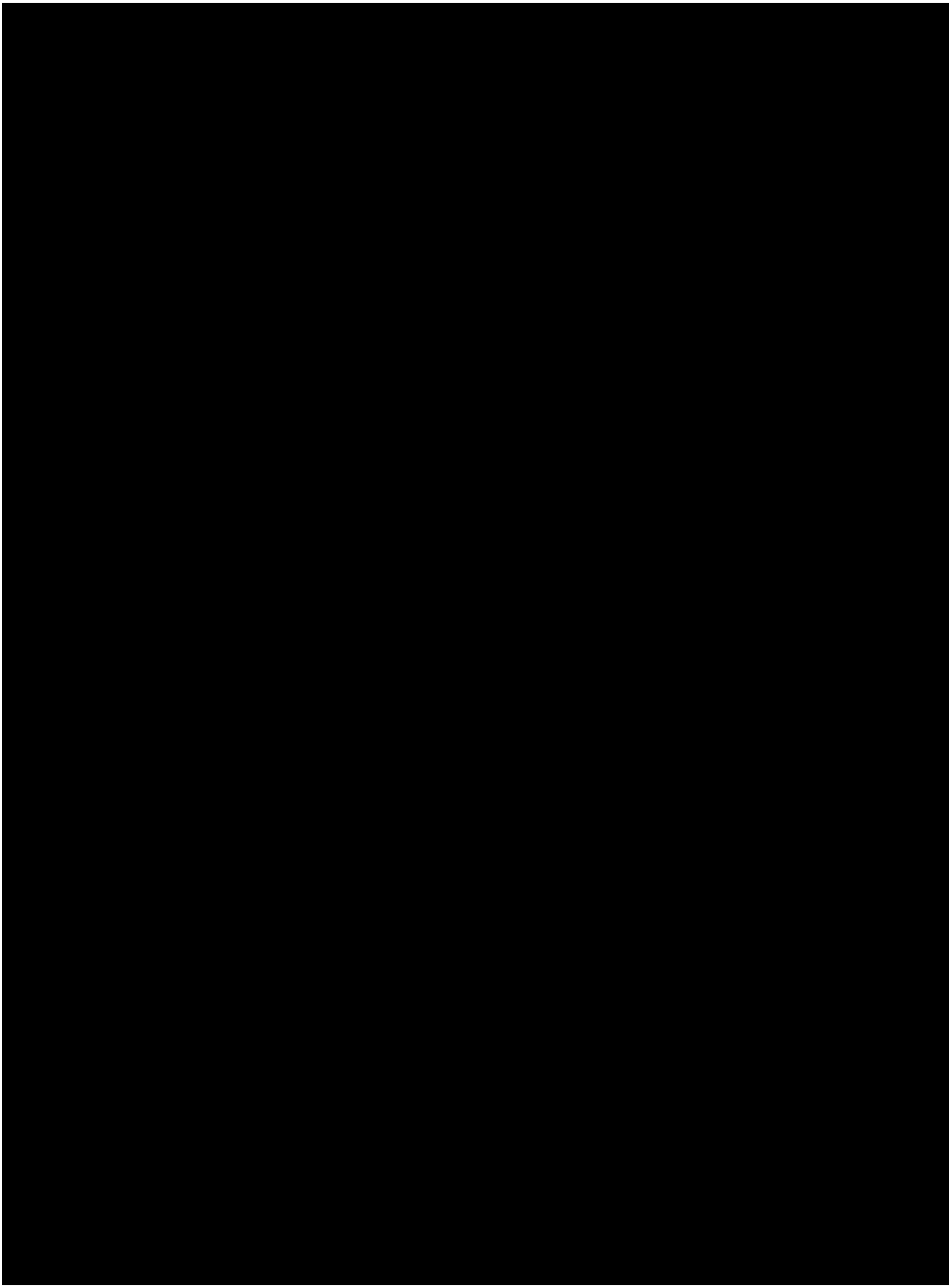


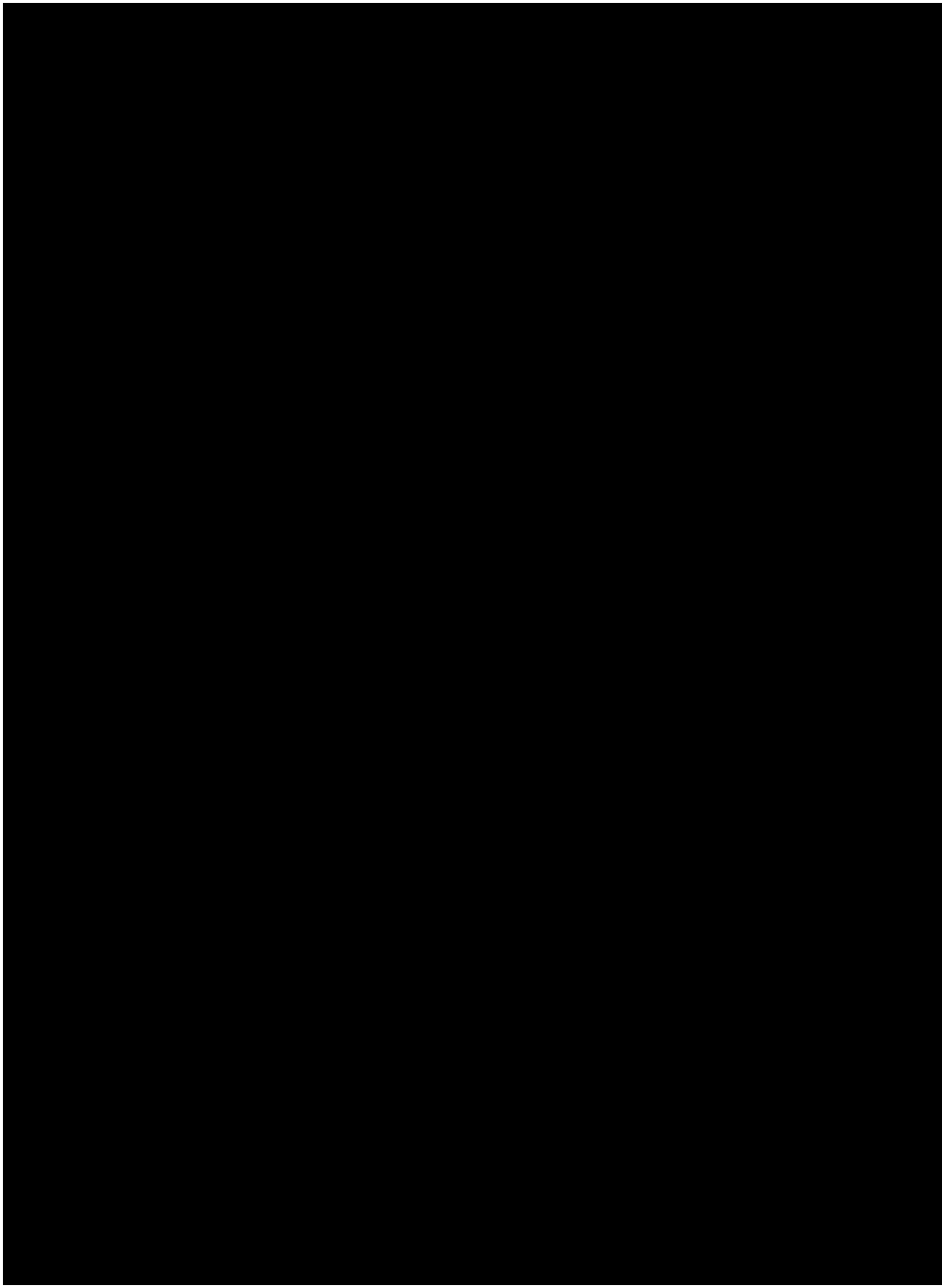


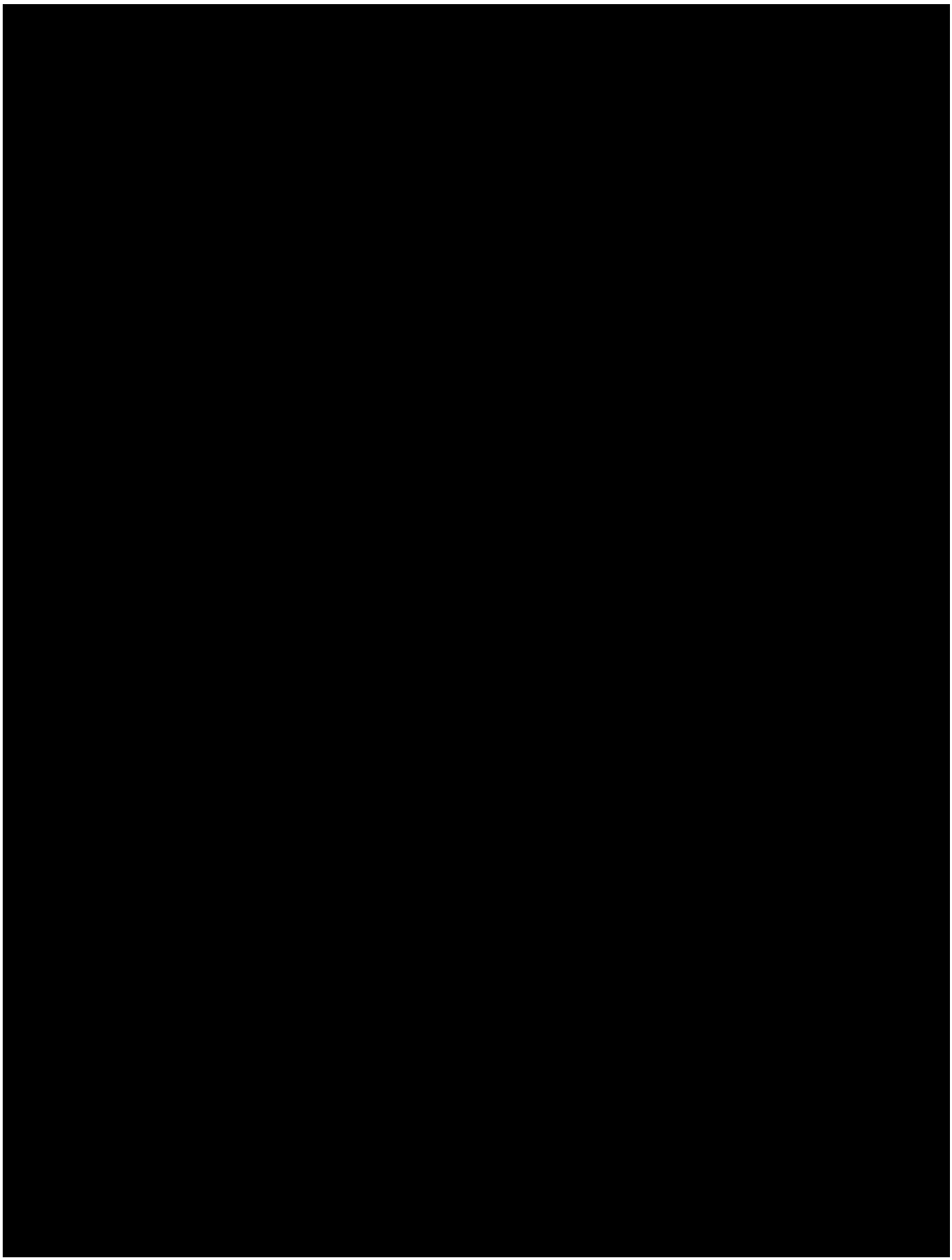


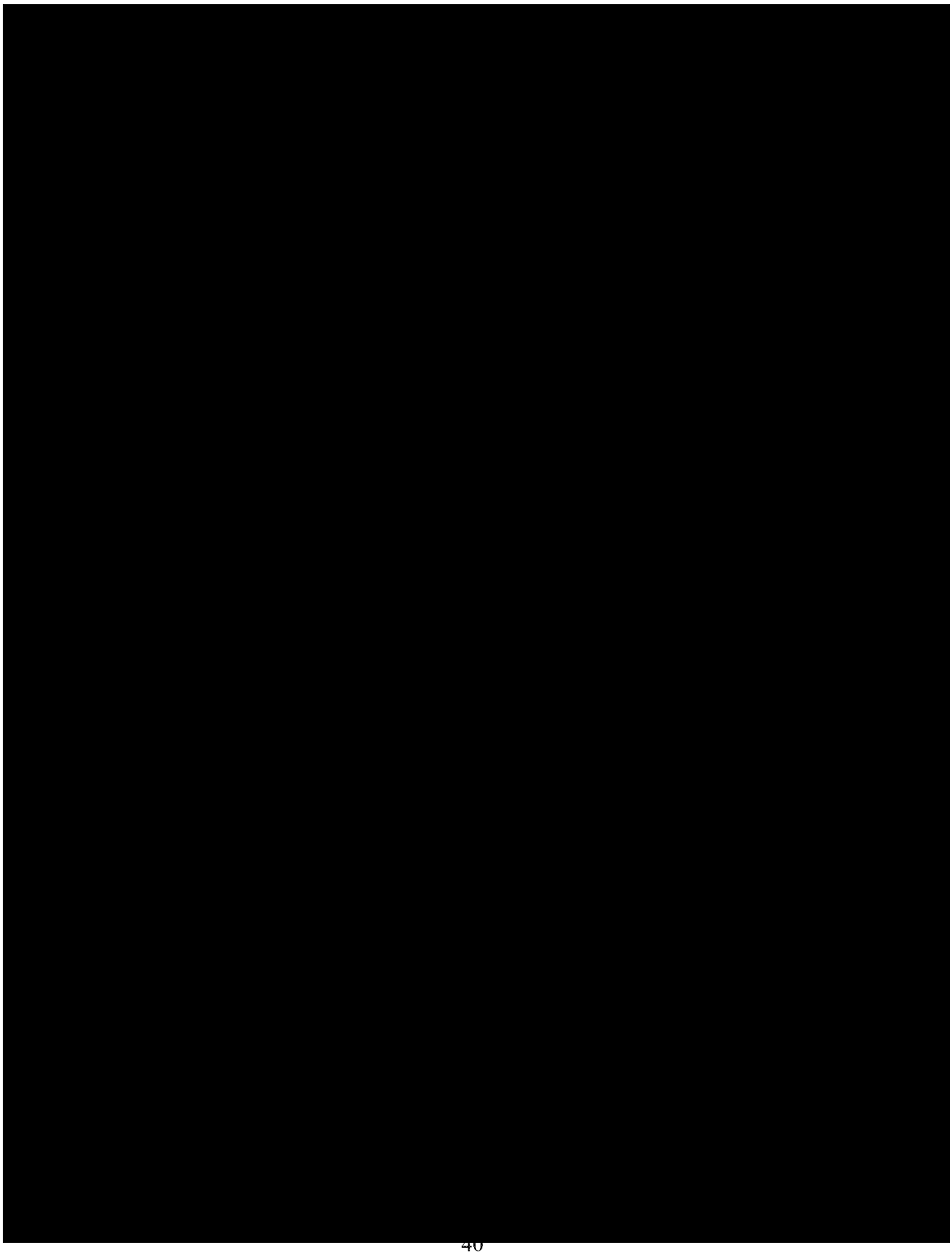


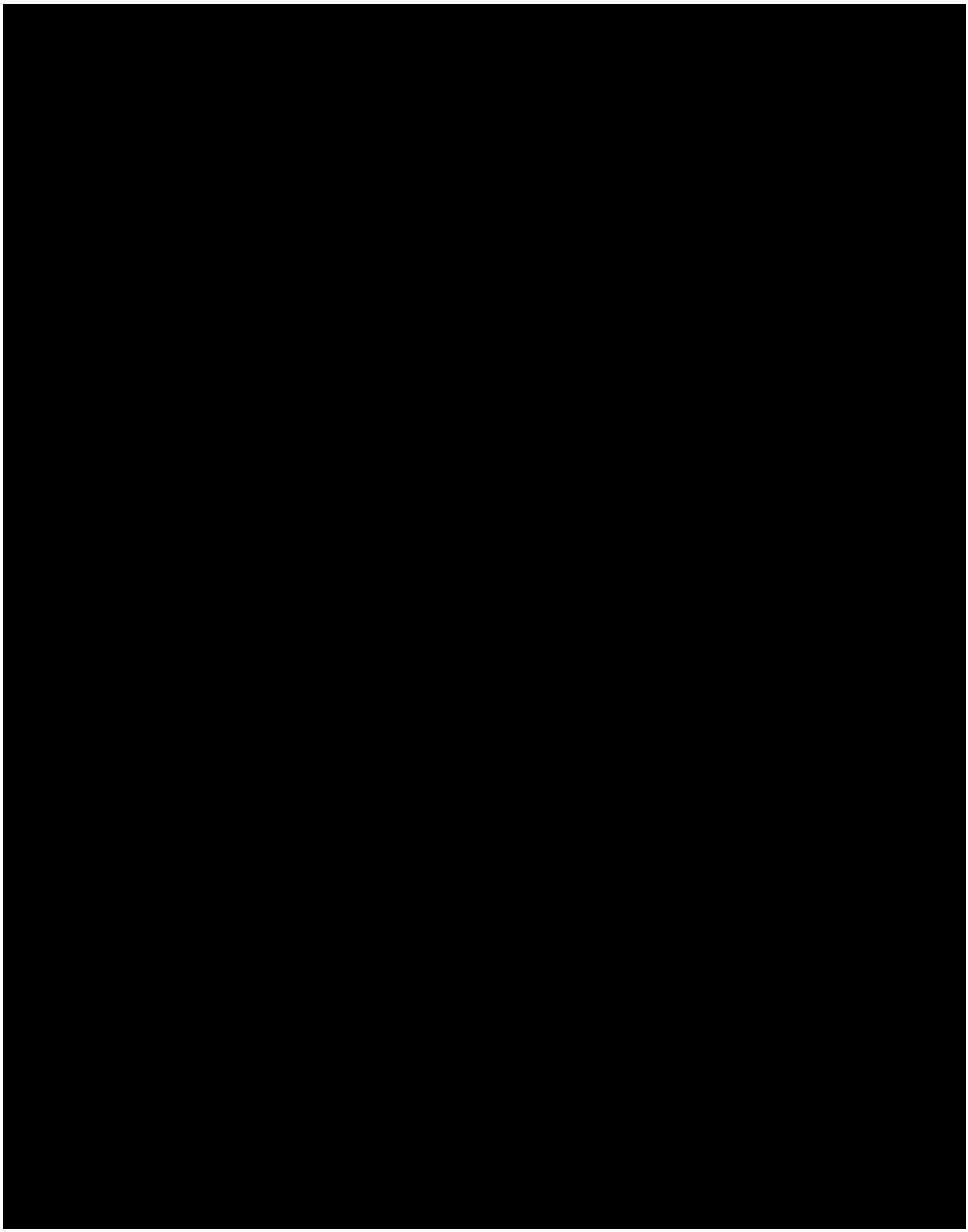


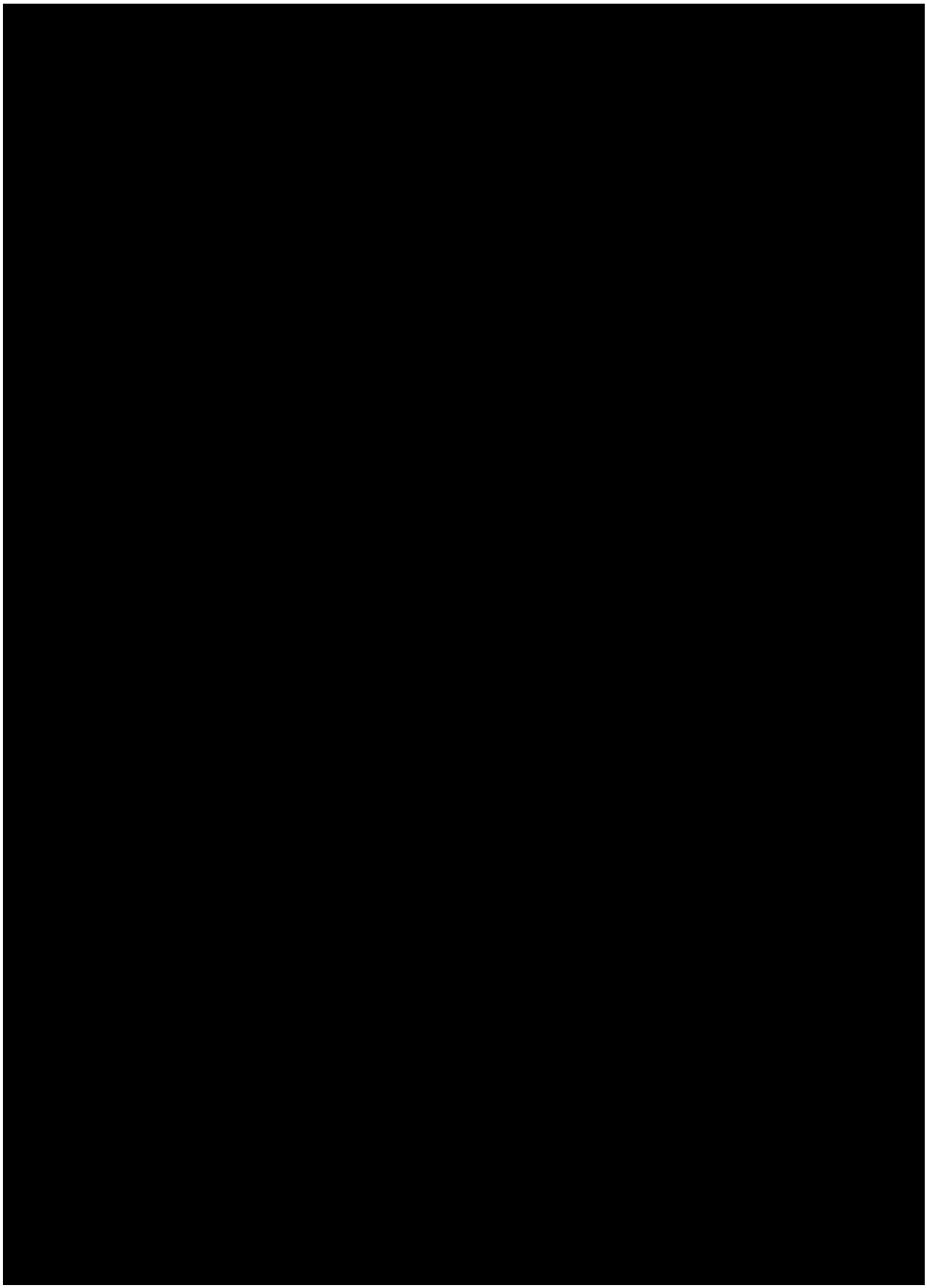


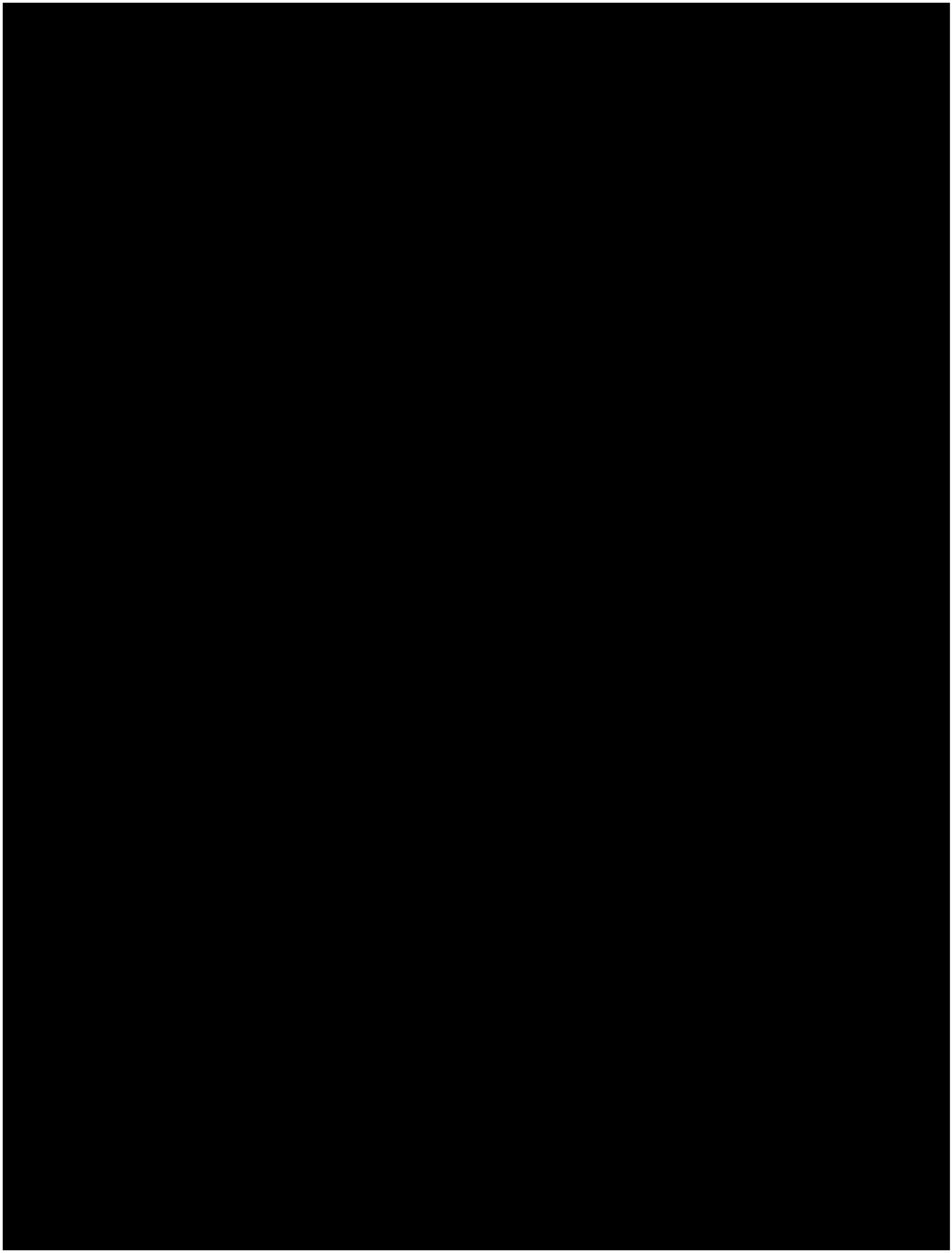


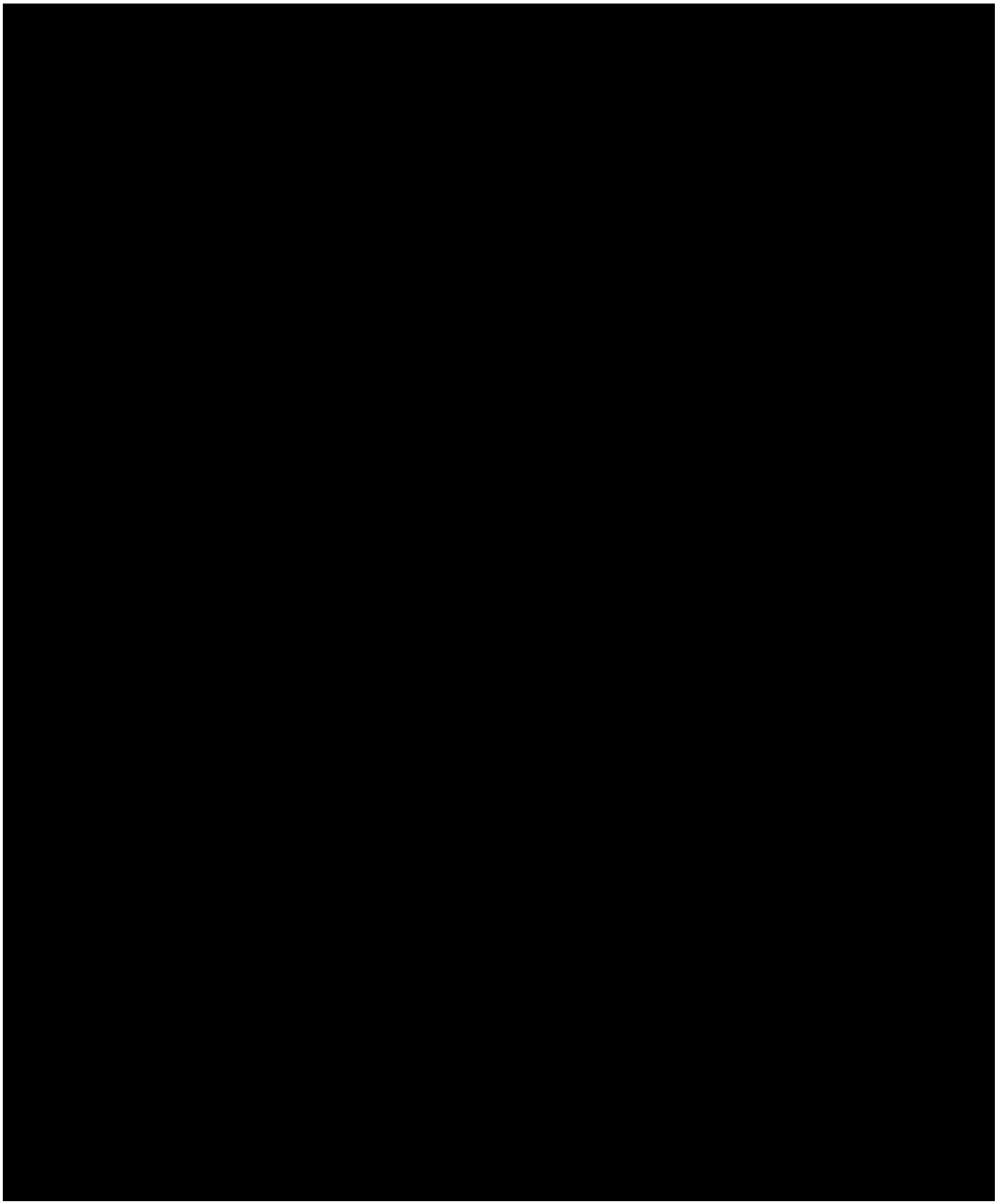












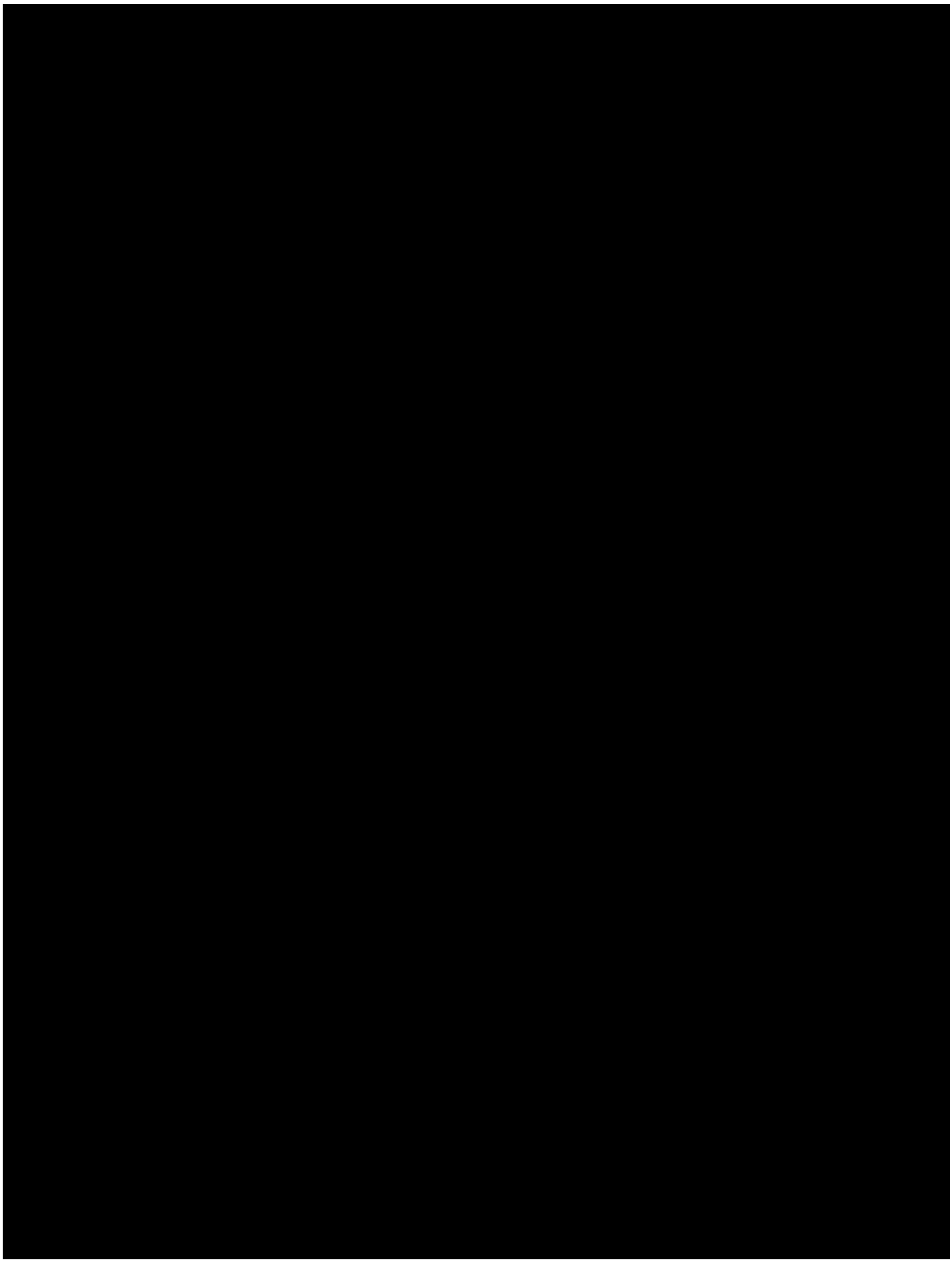
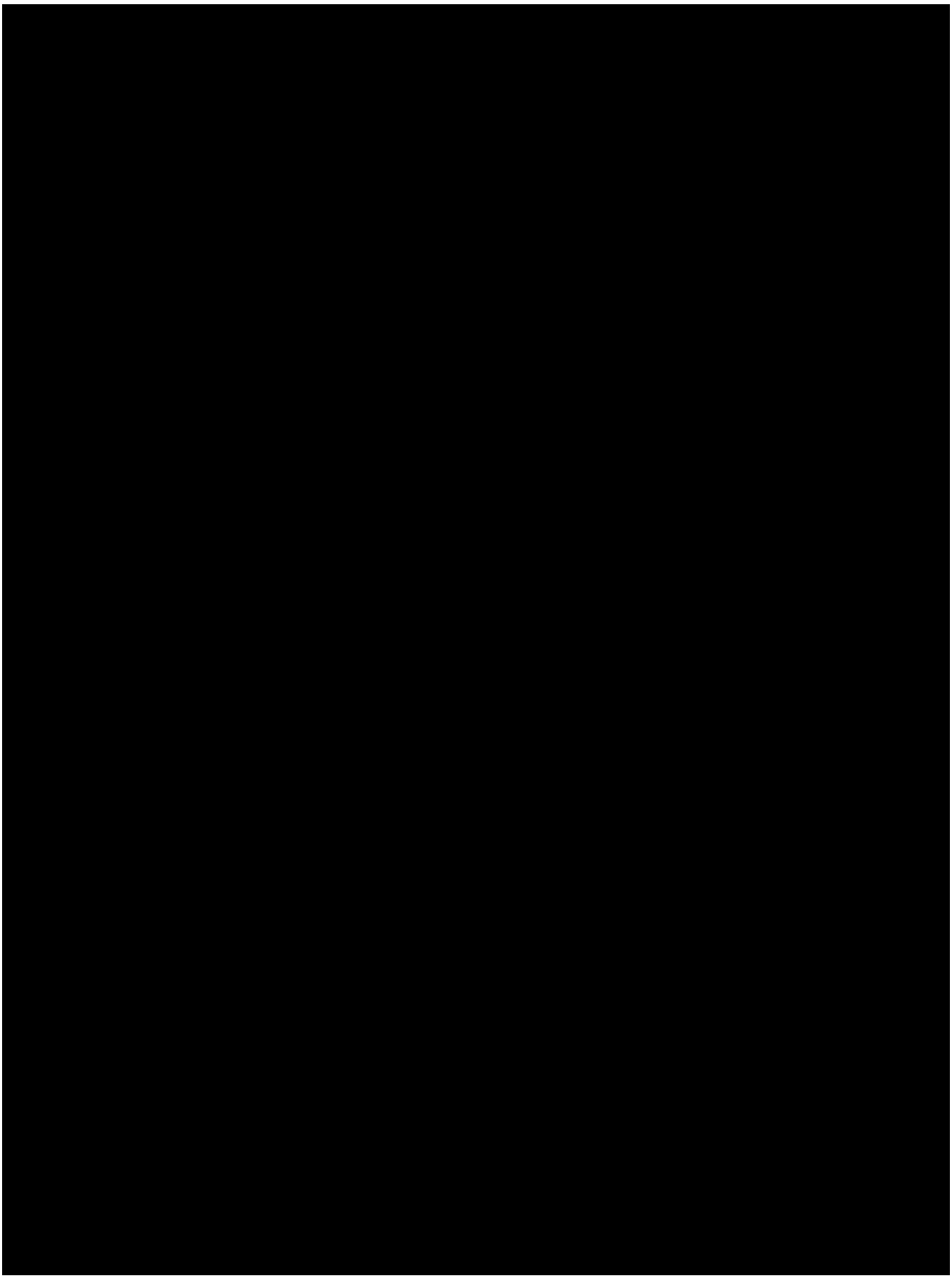
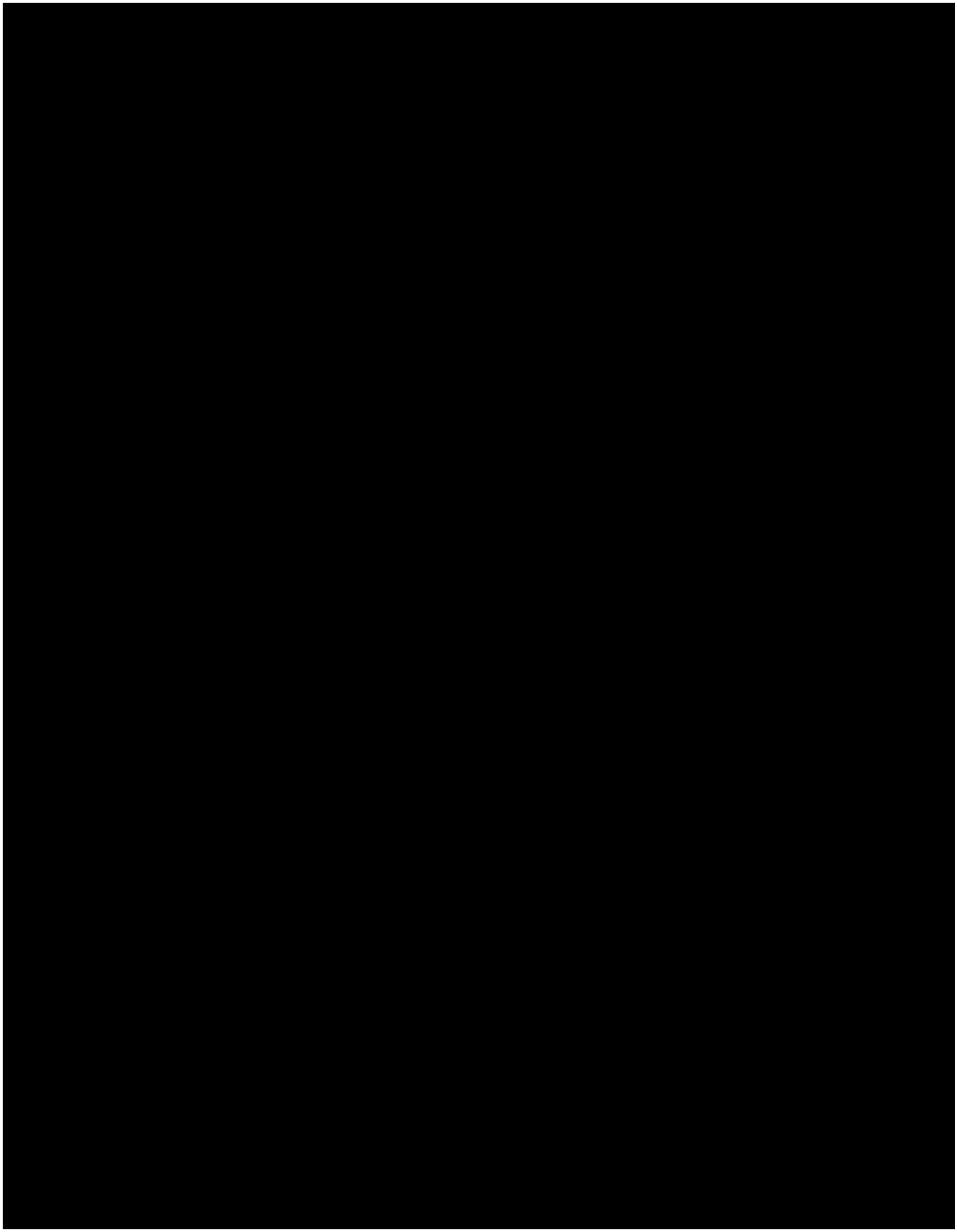
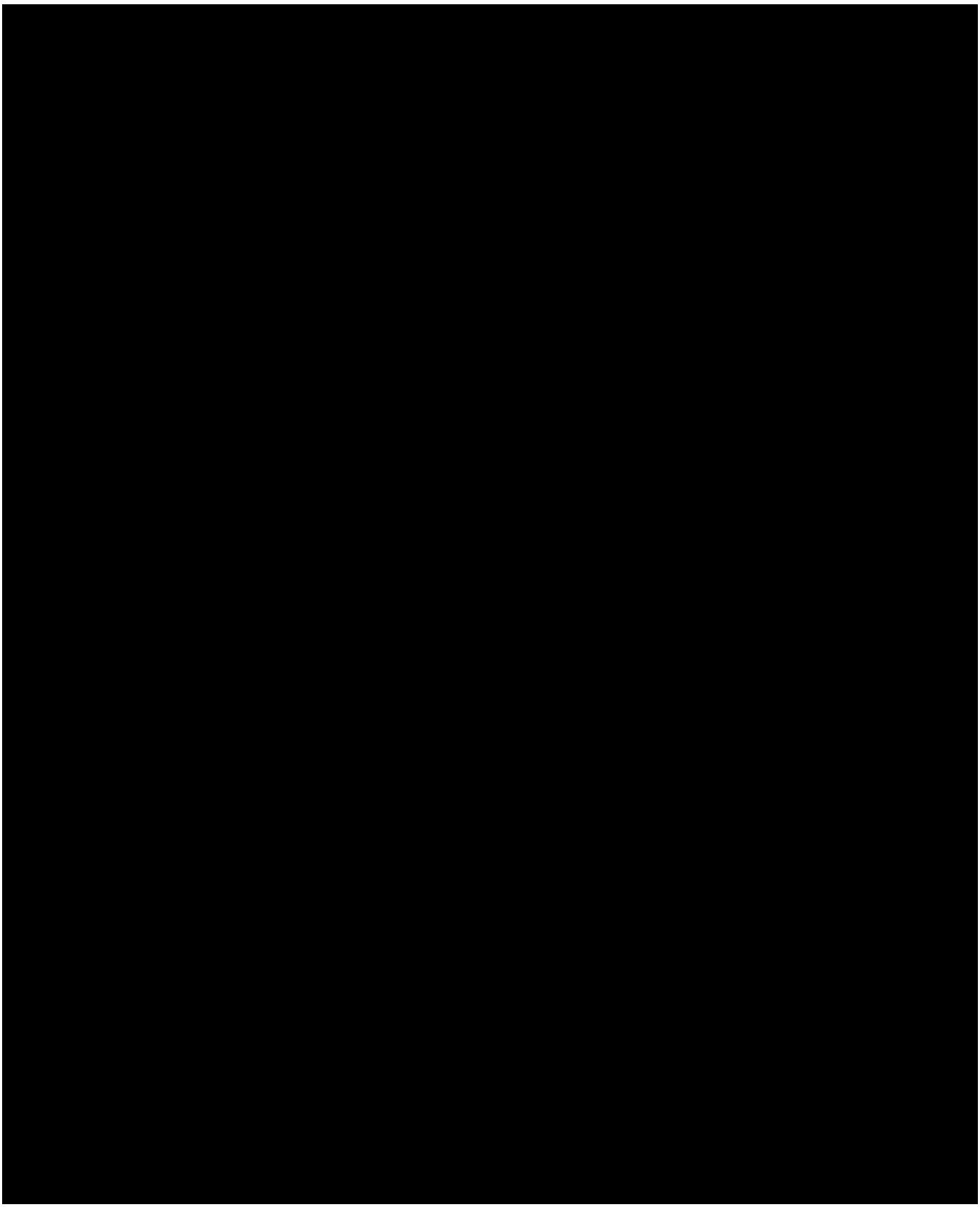
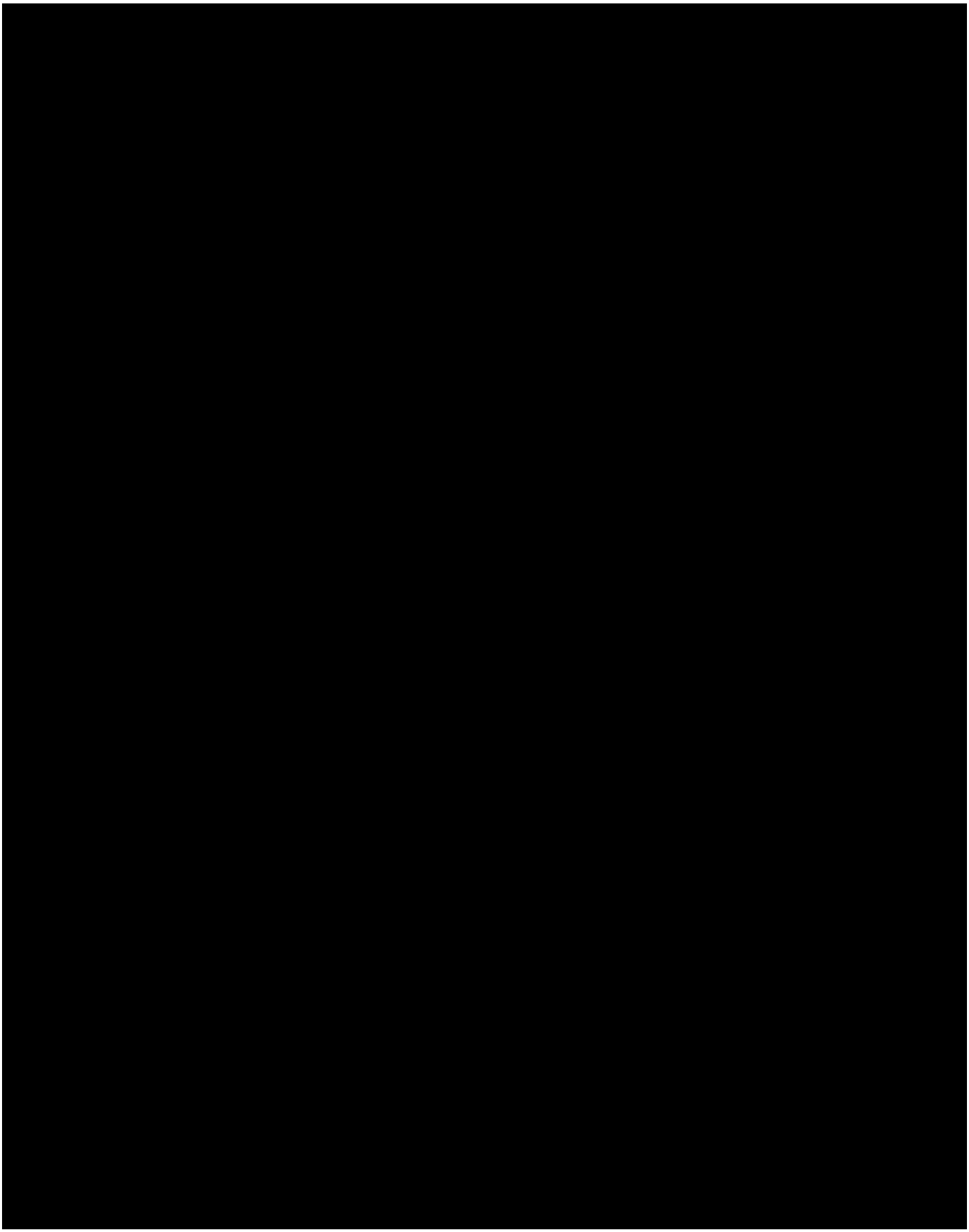


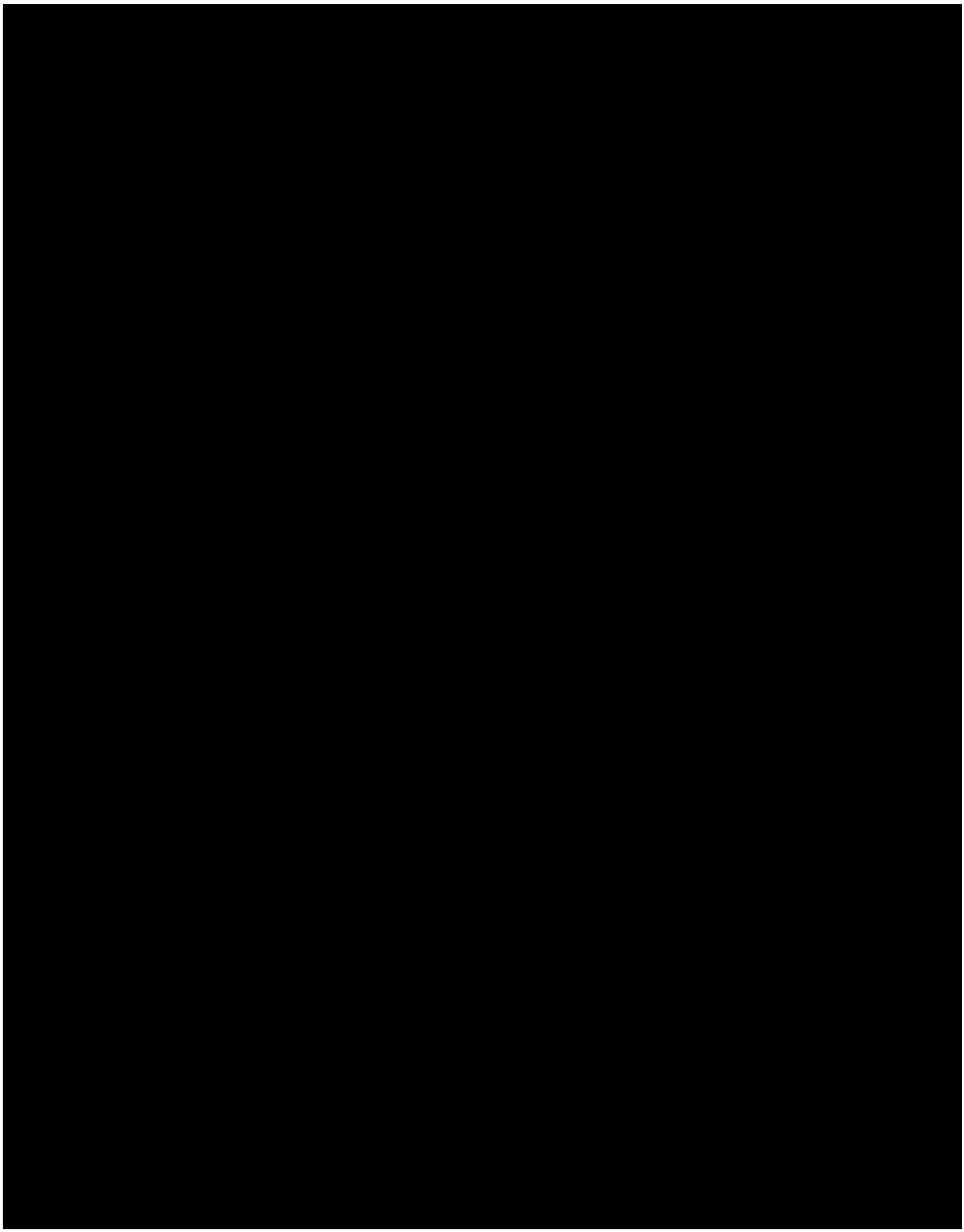
Exhibit A

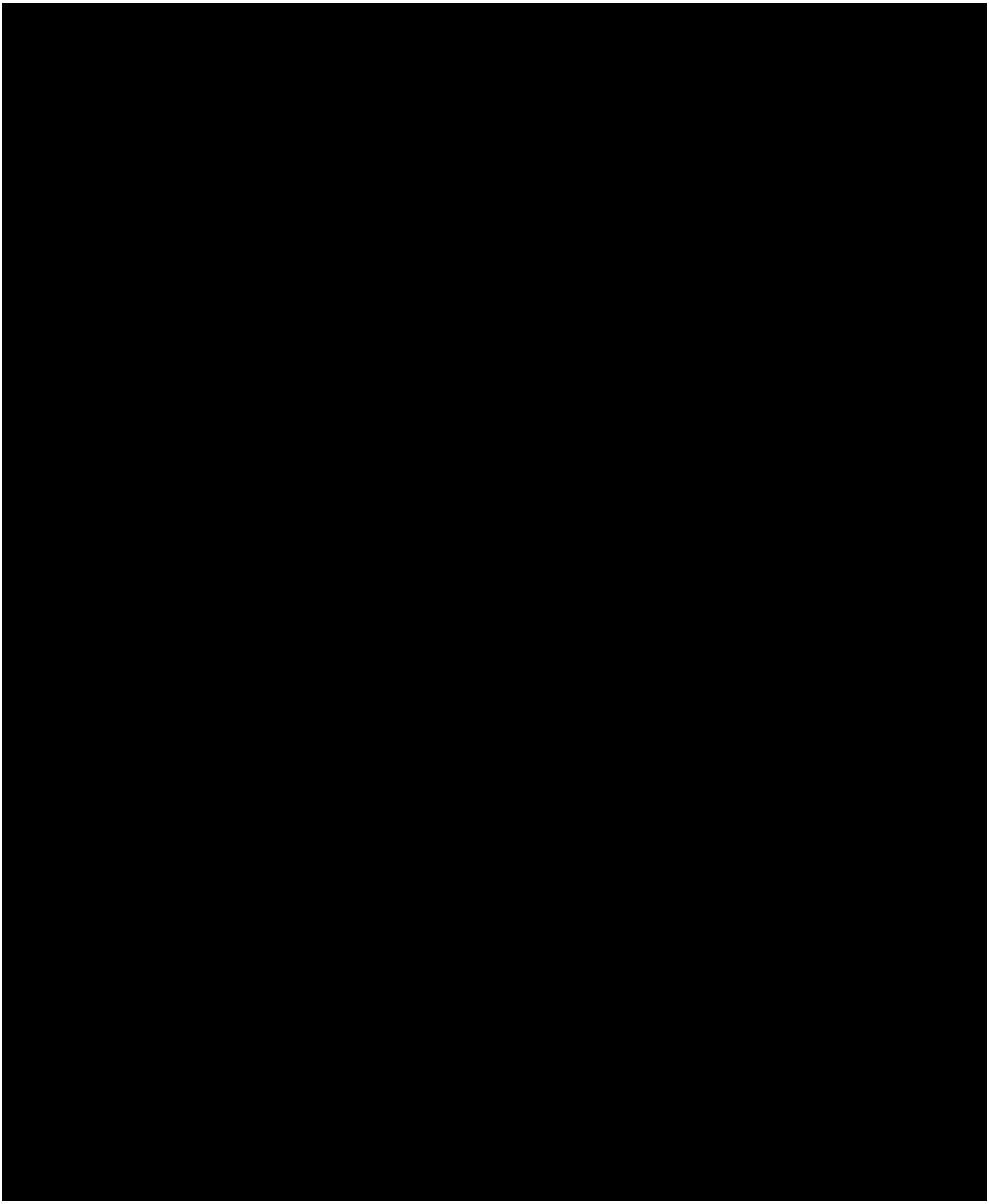


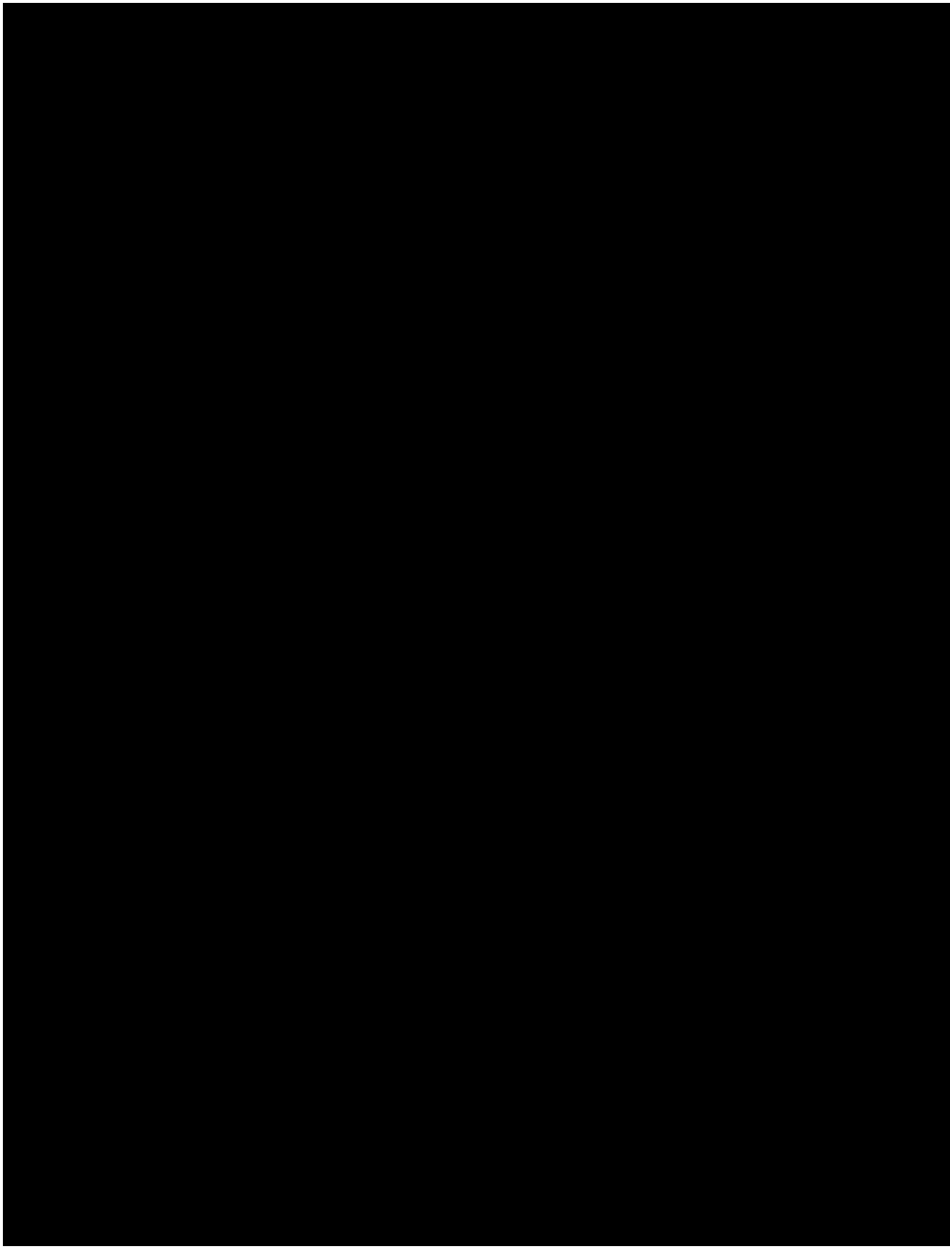


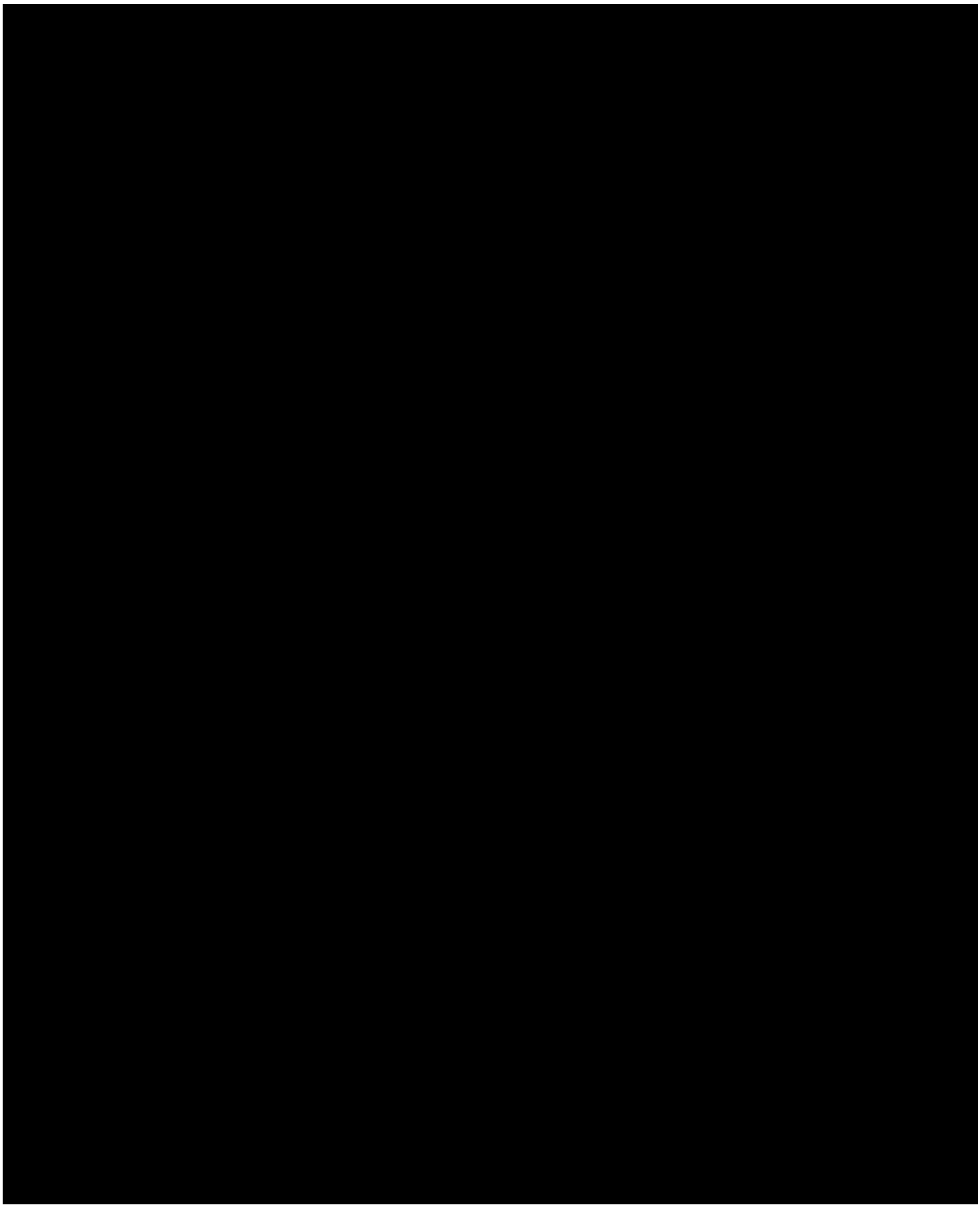


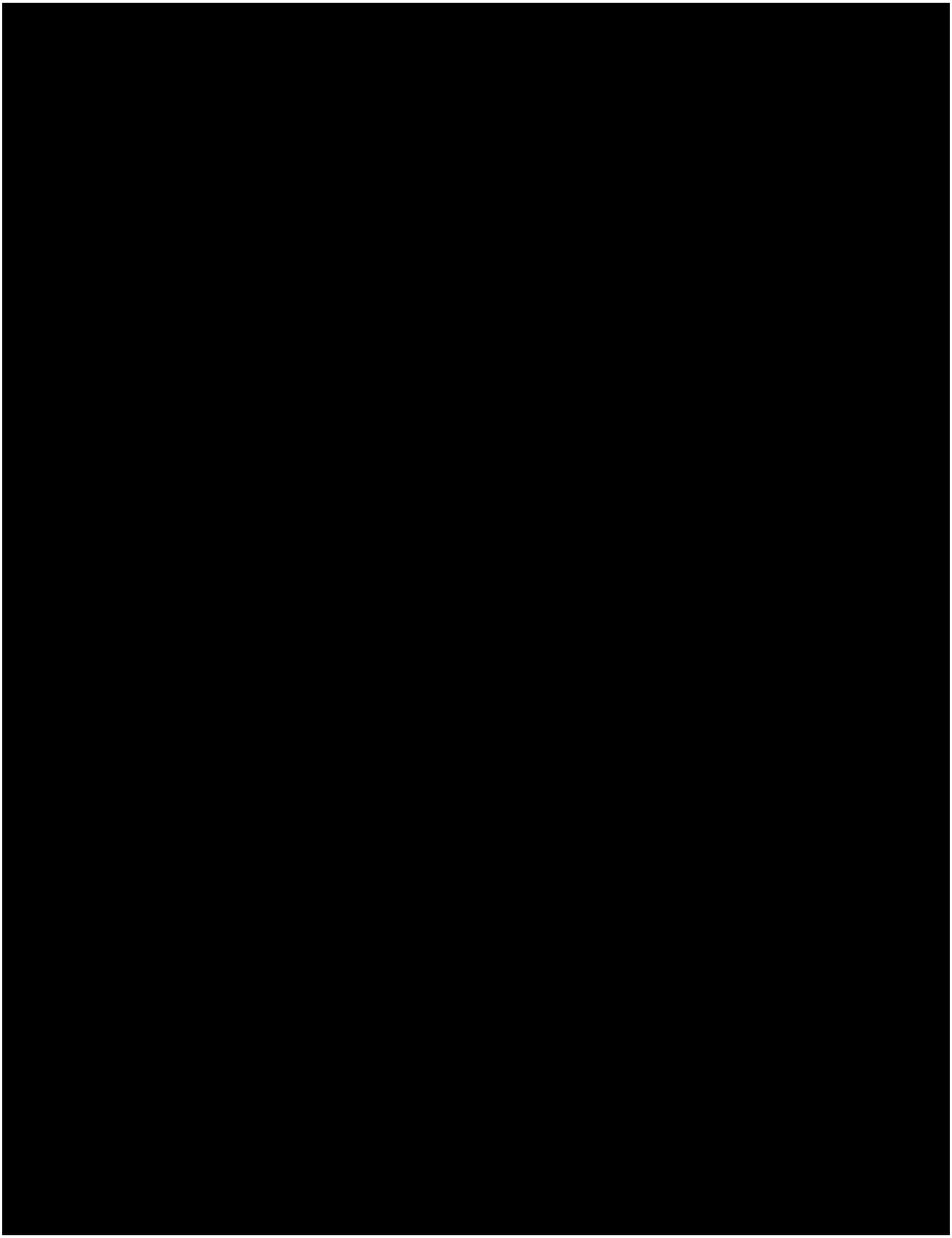


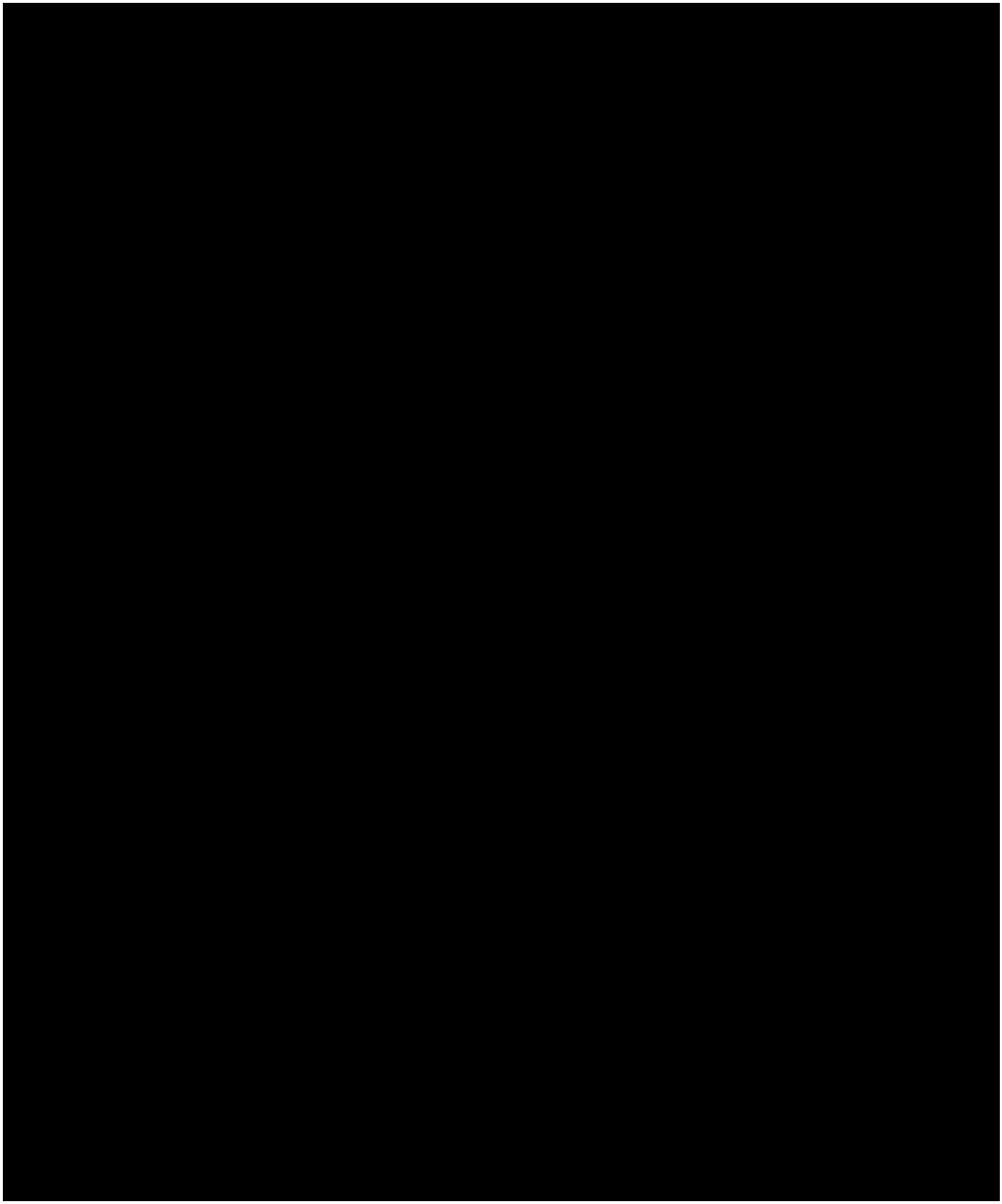


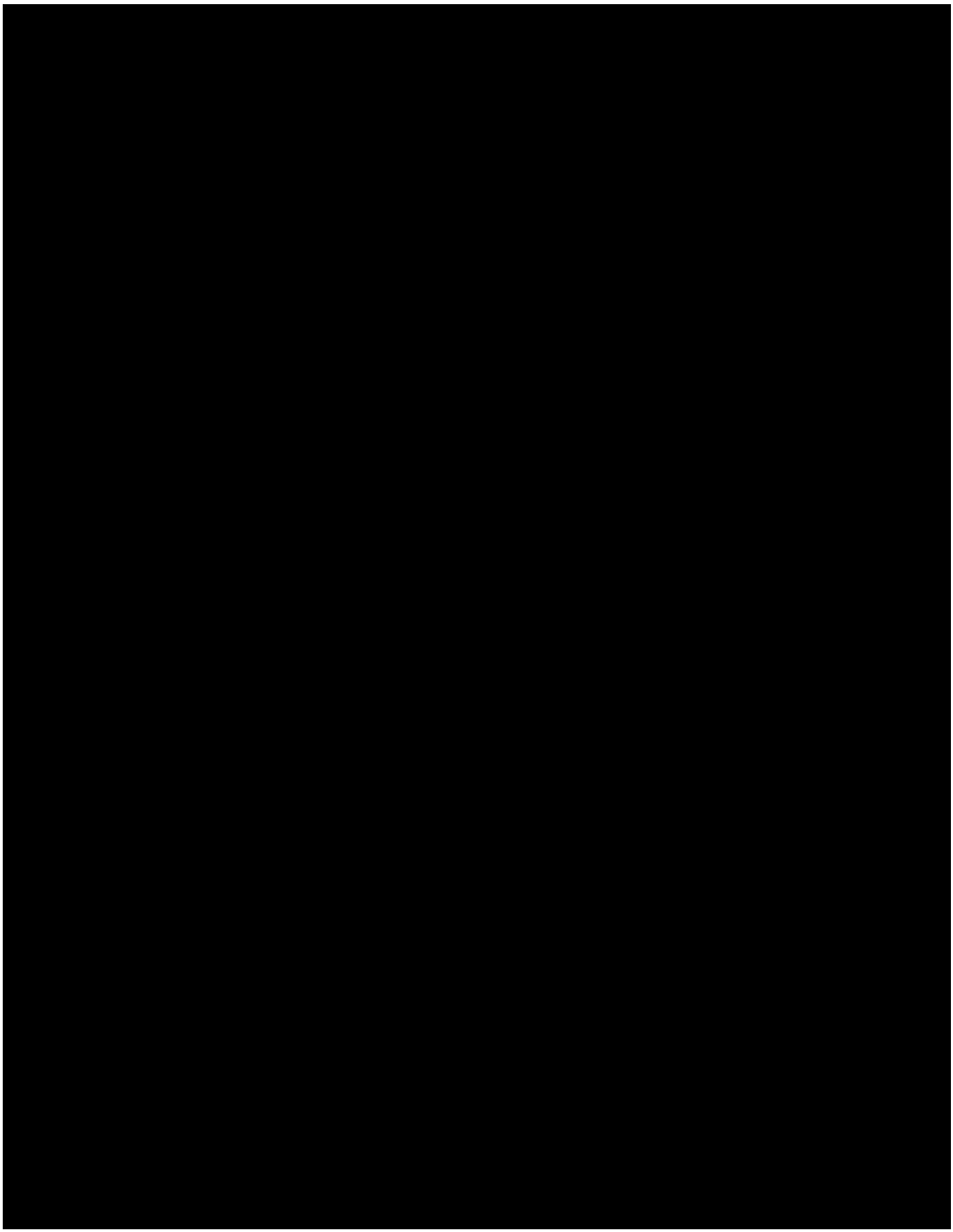


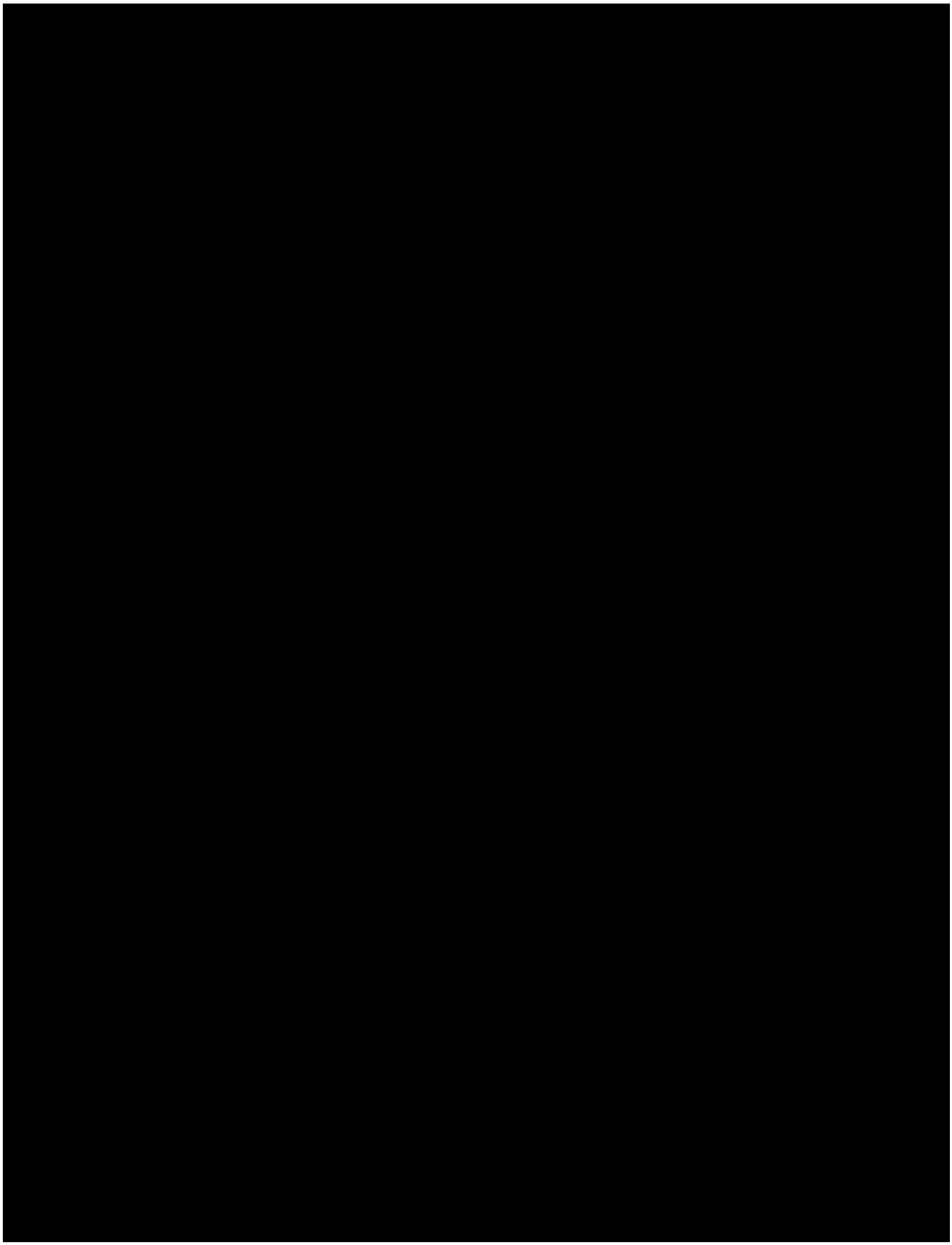


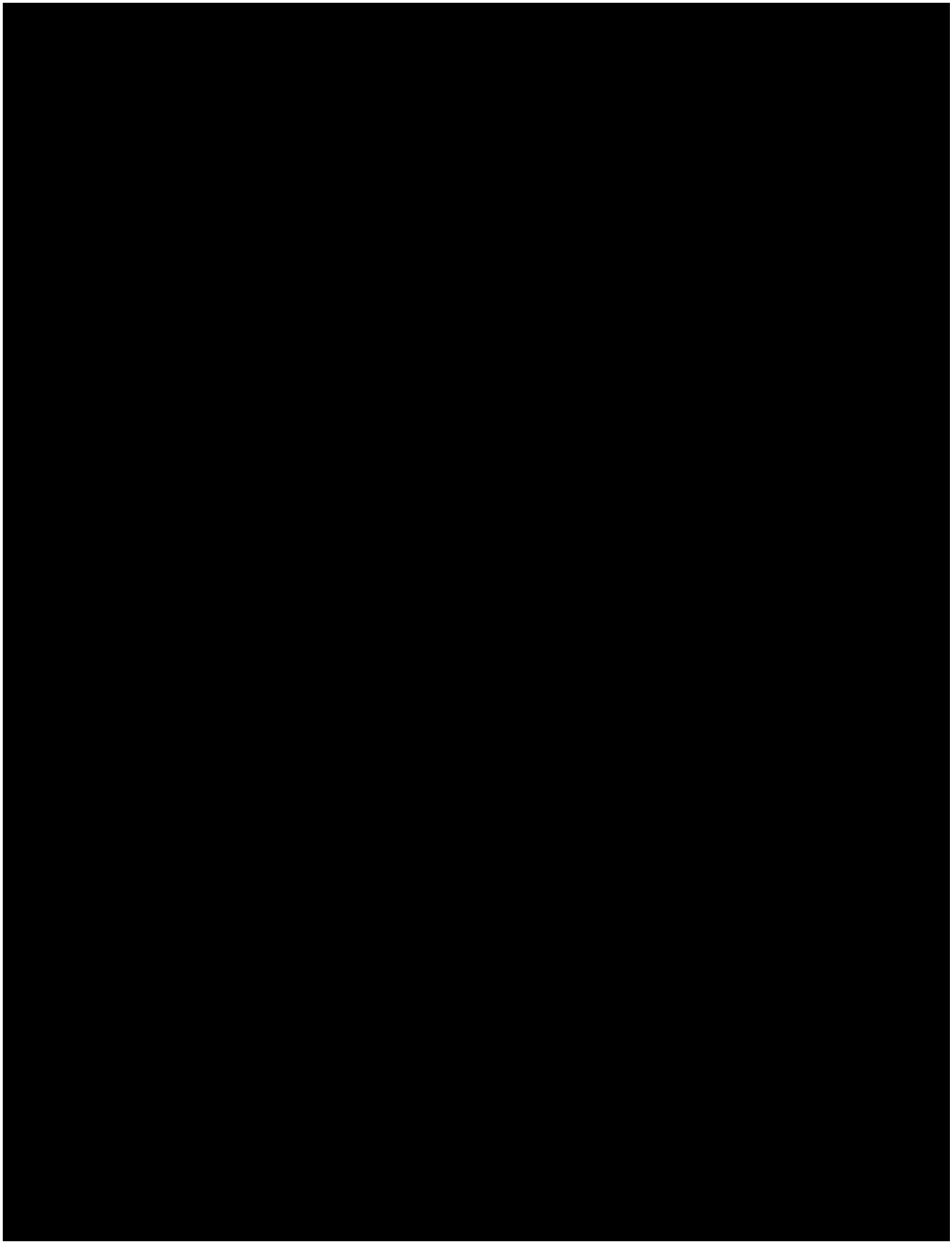


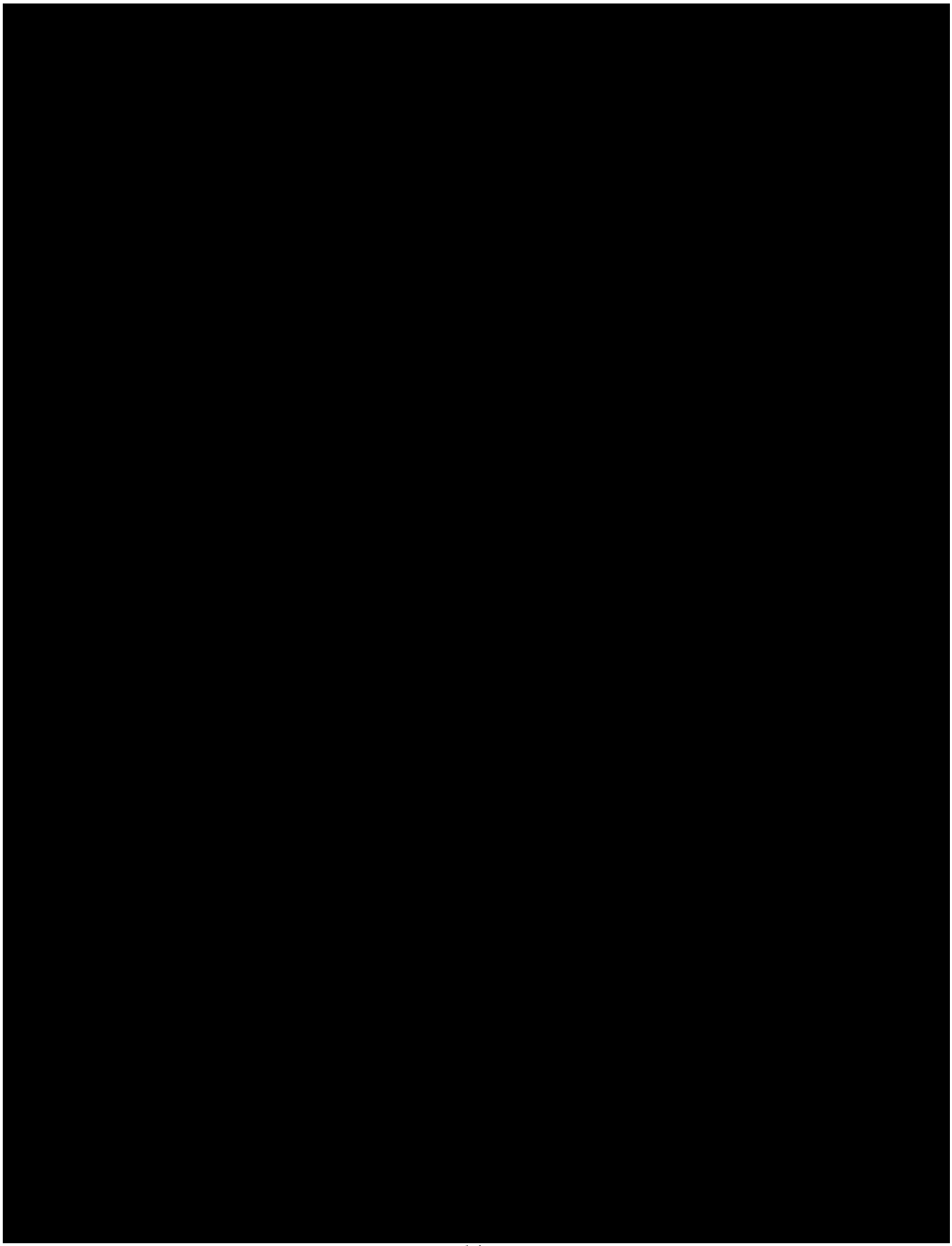


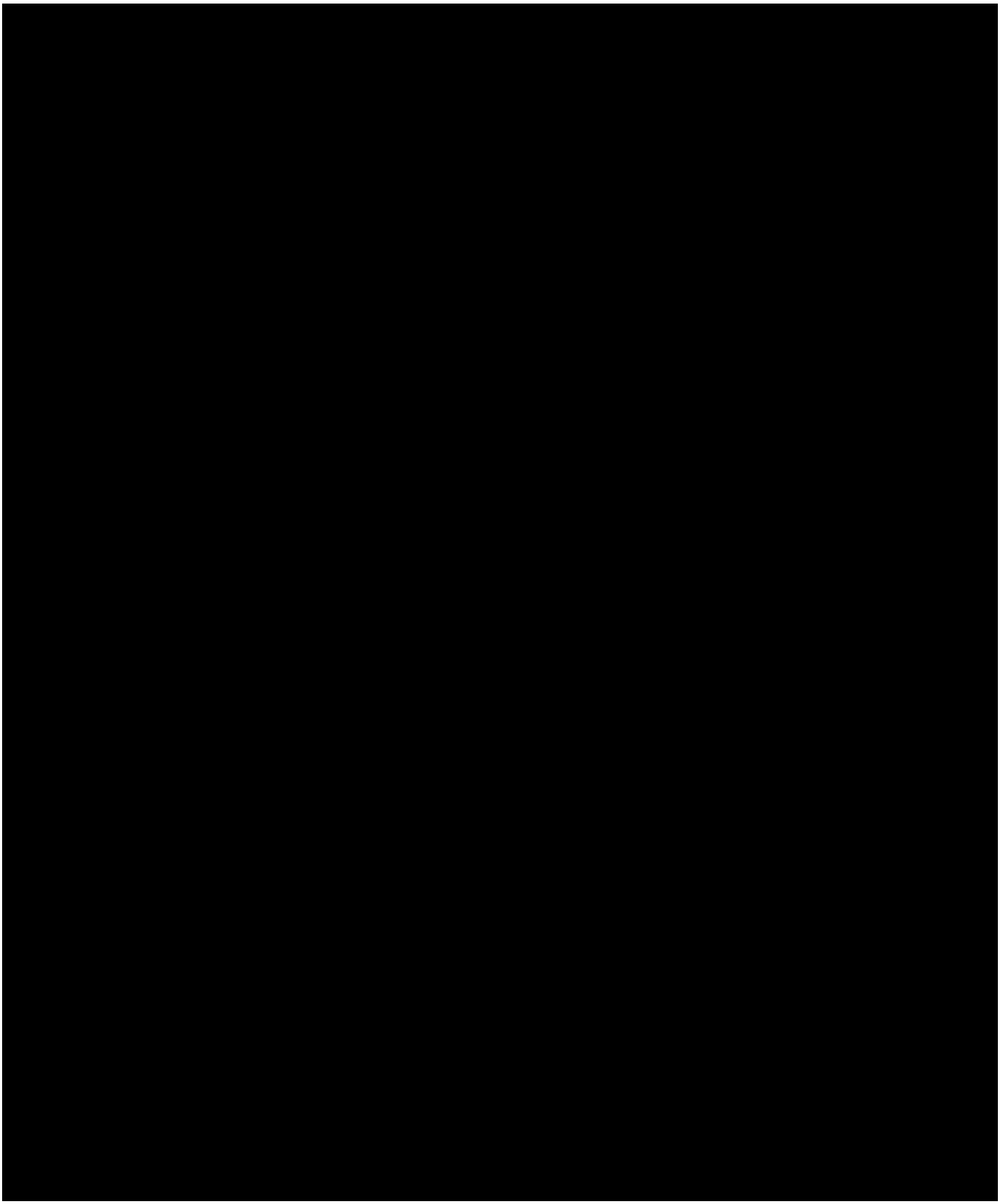


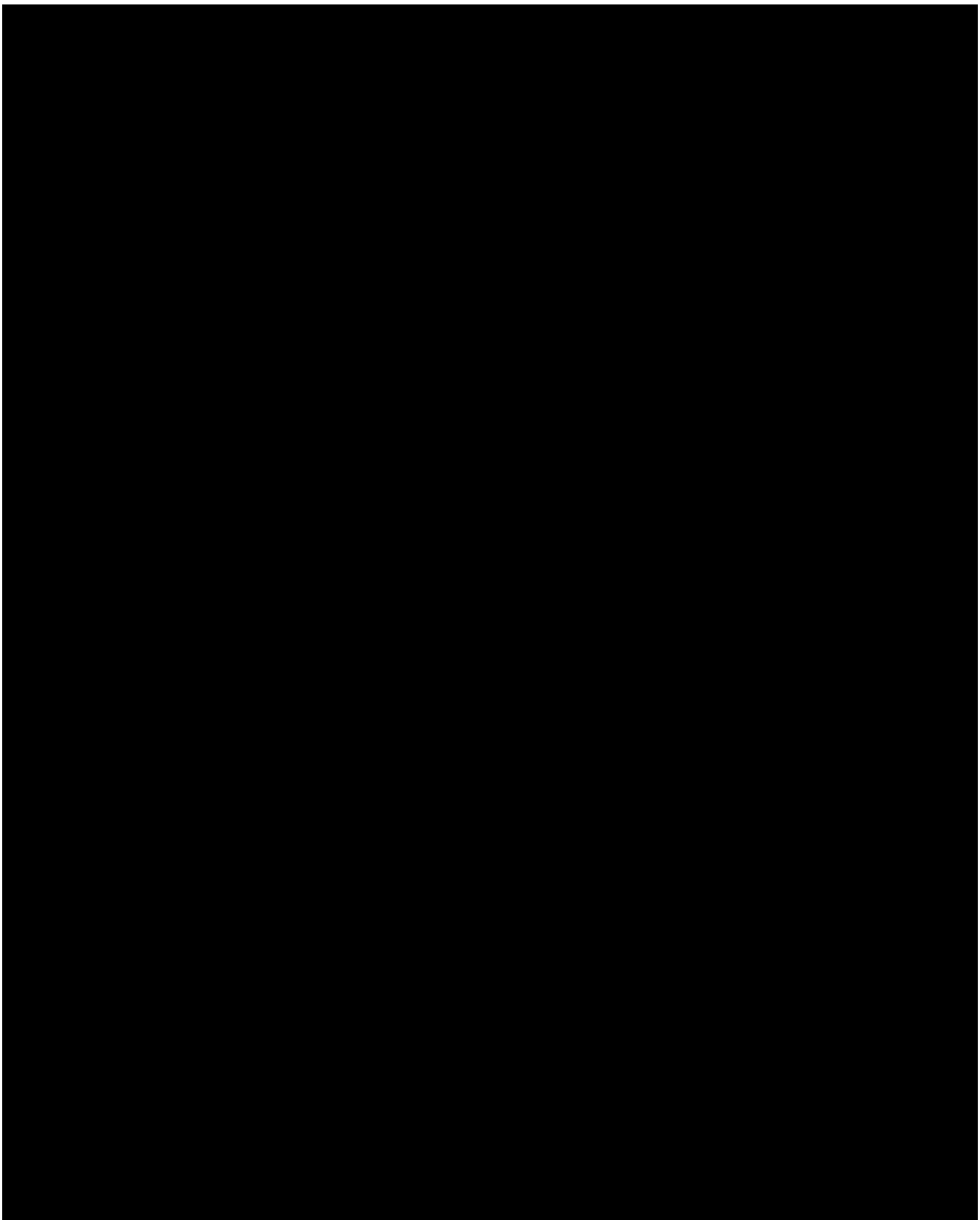




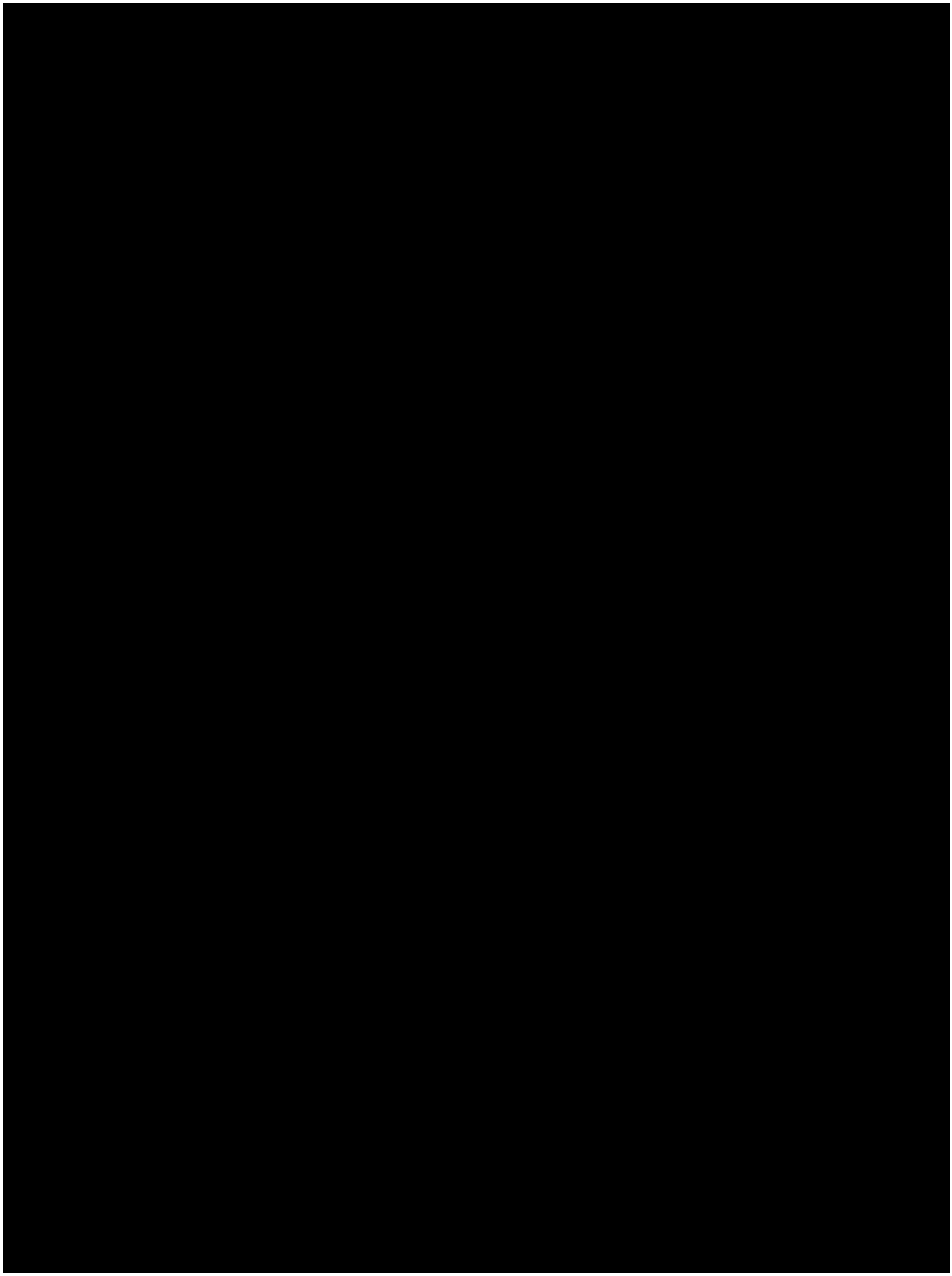


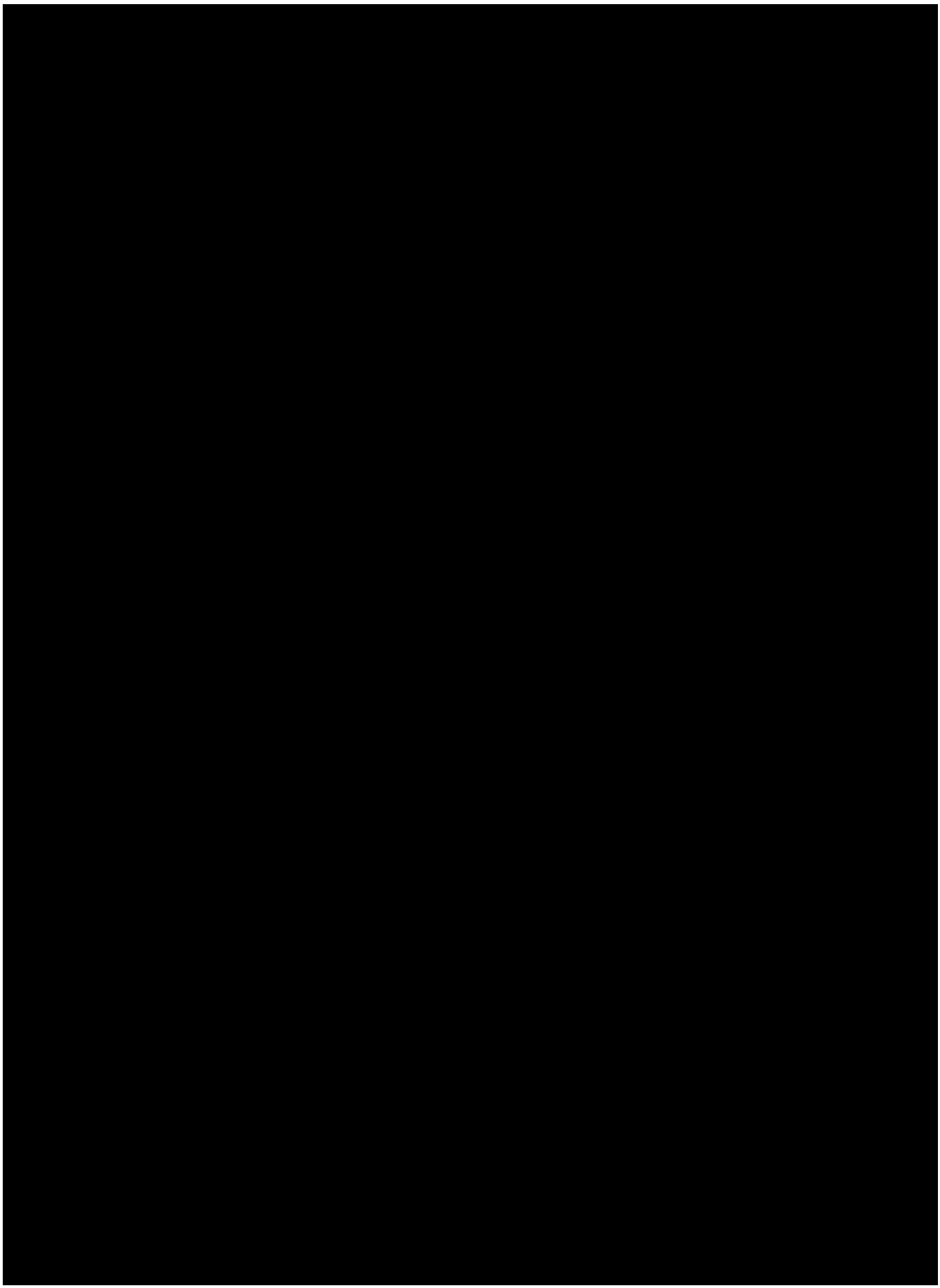


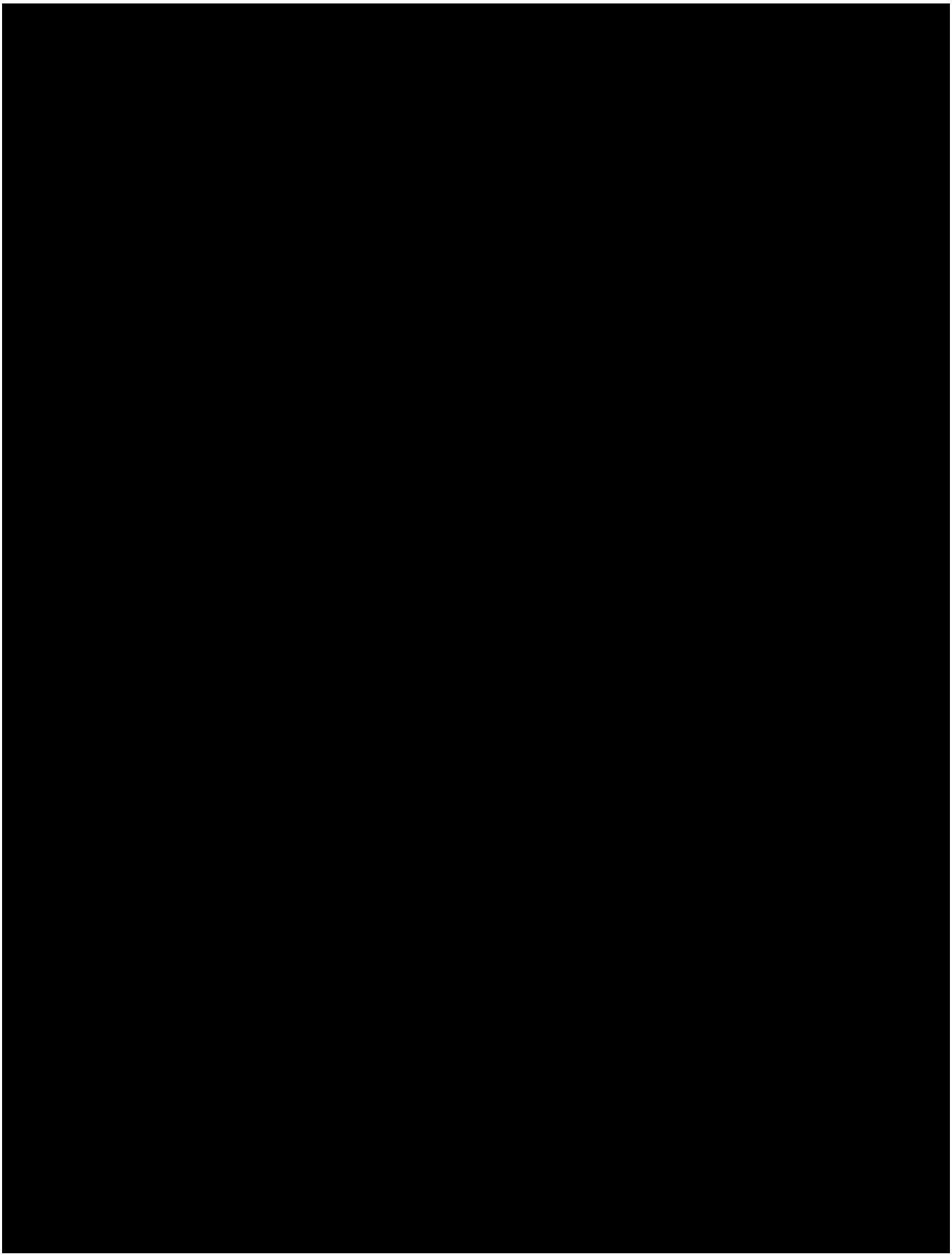


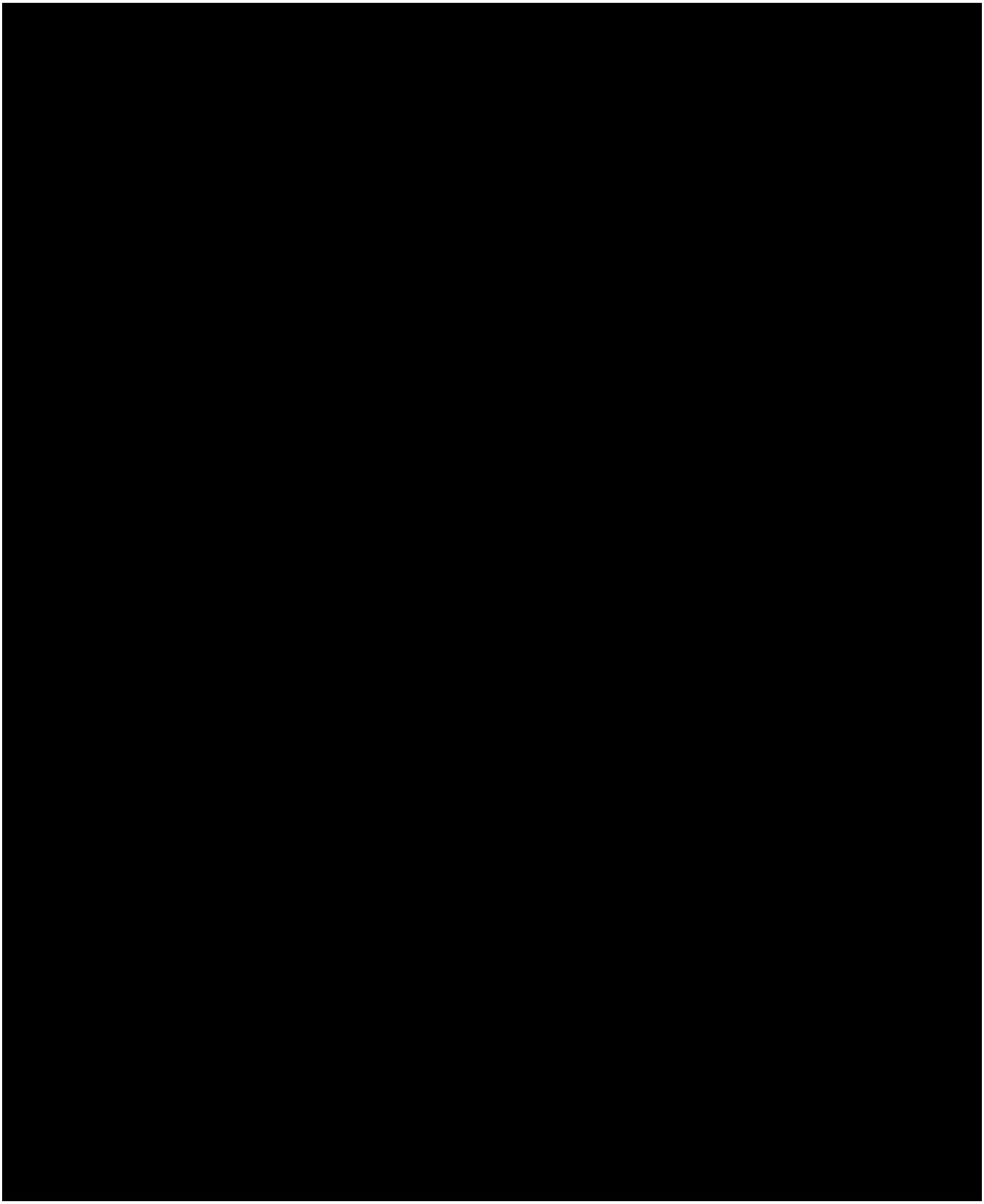


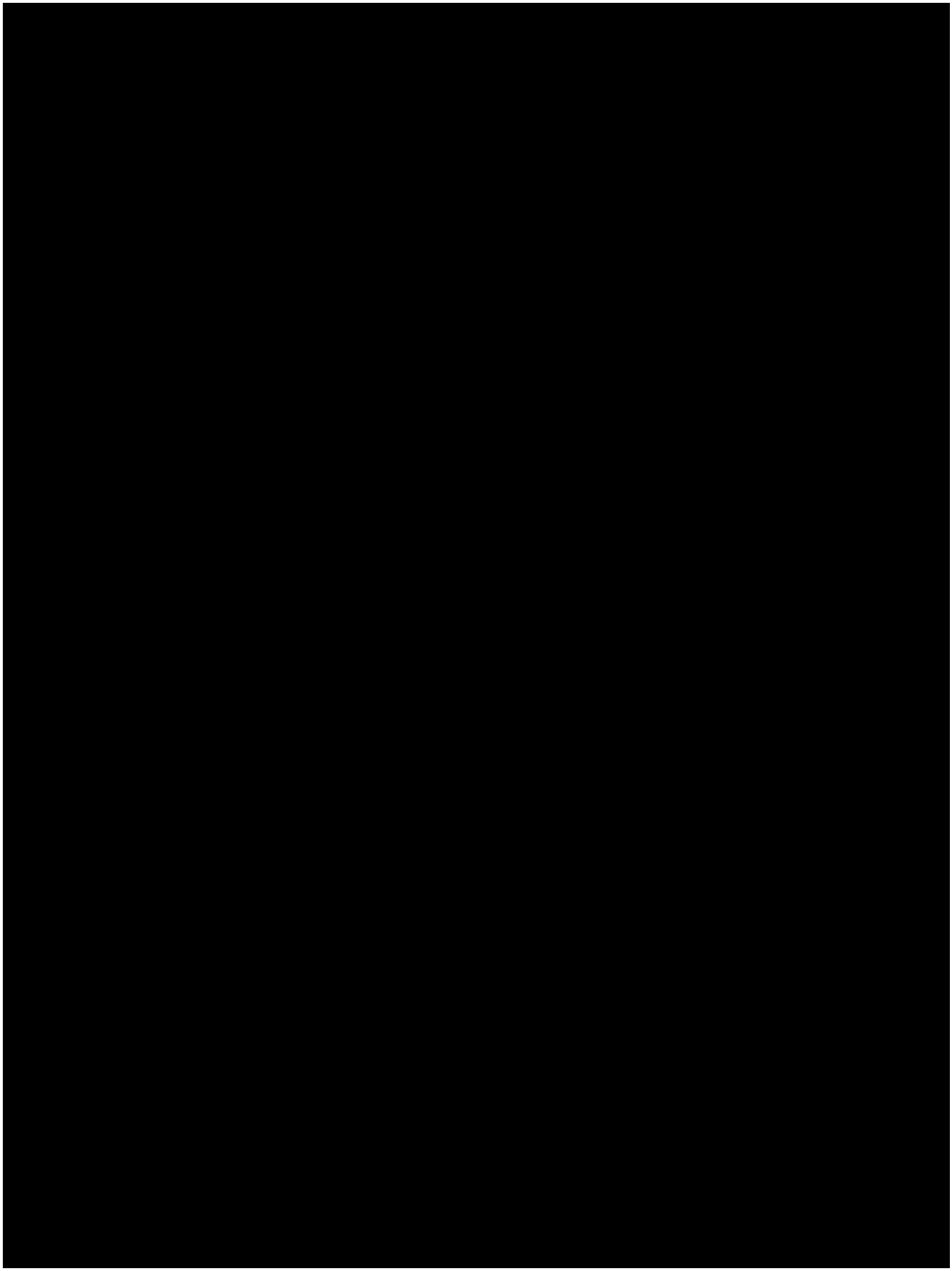
12.06.2018

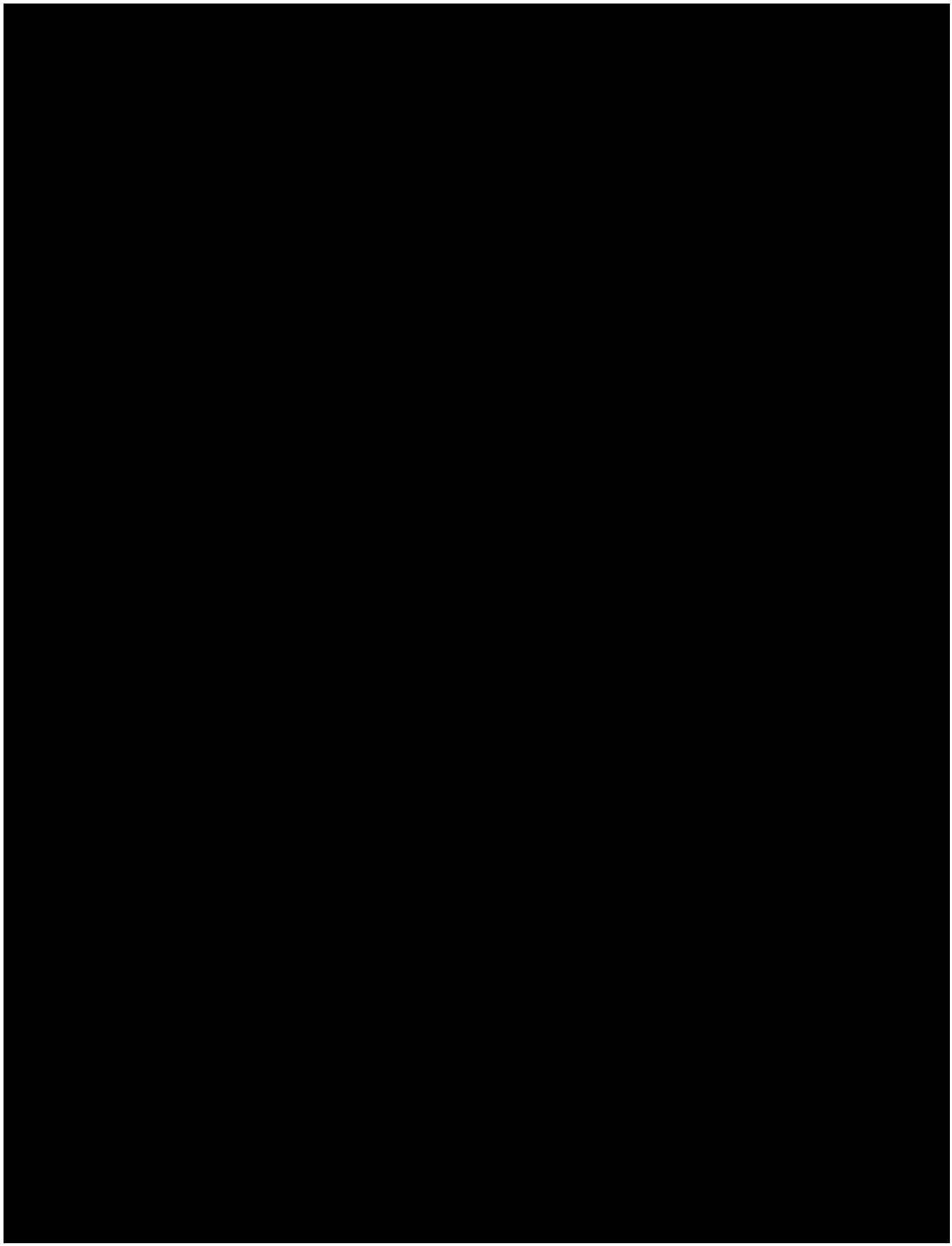


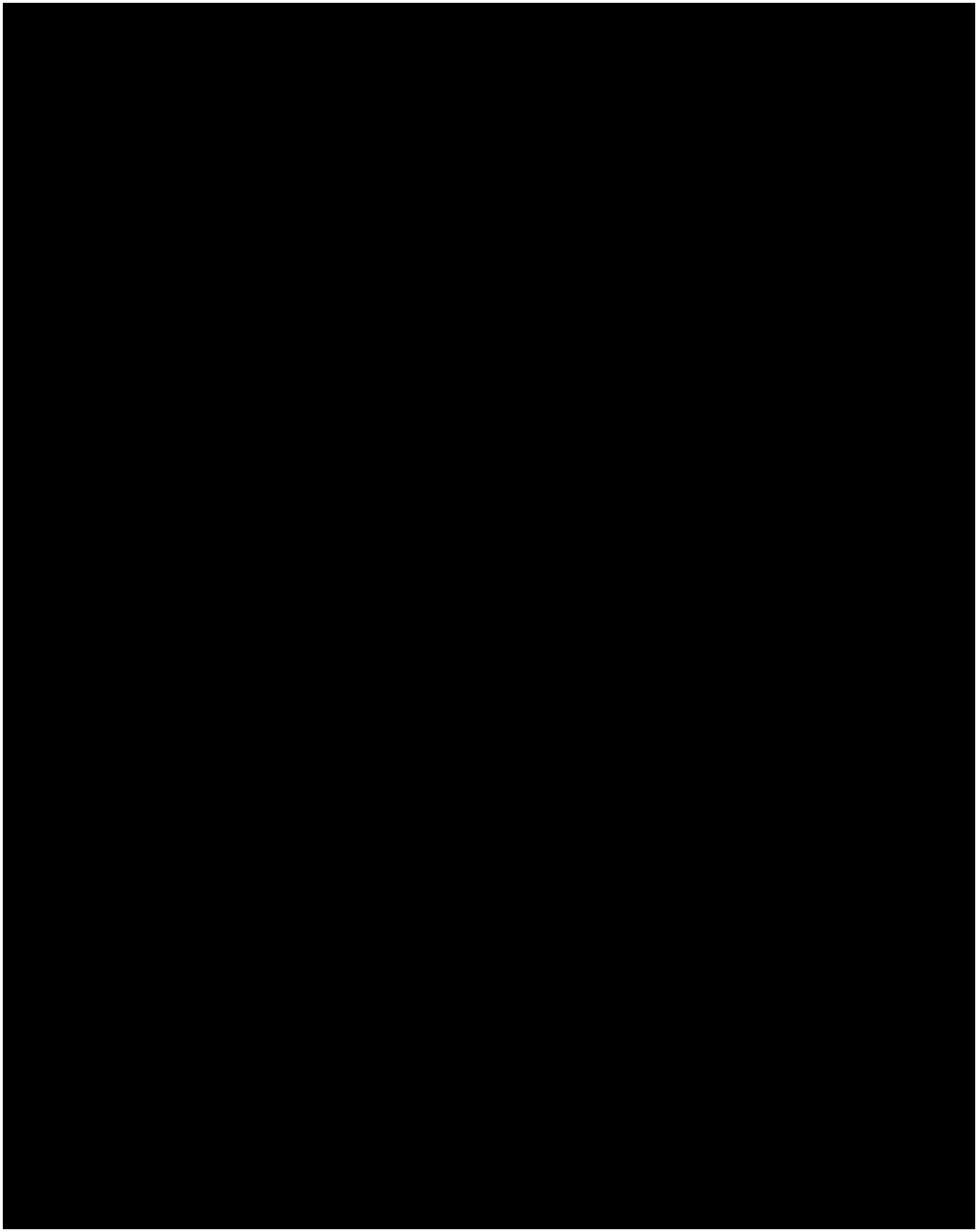


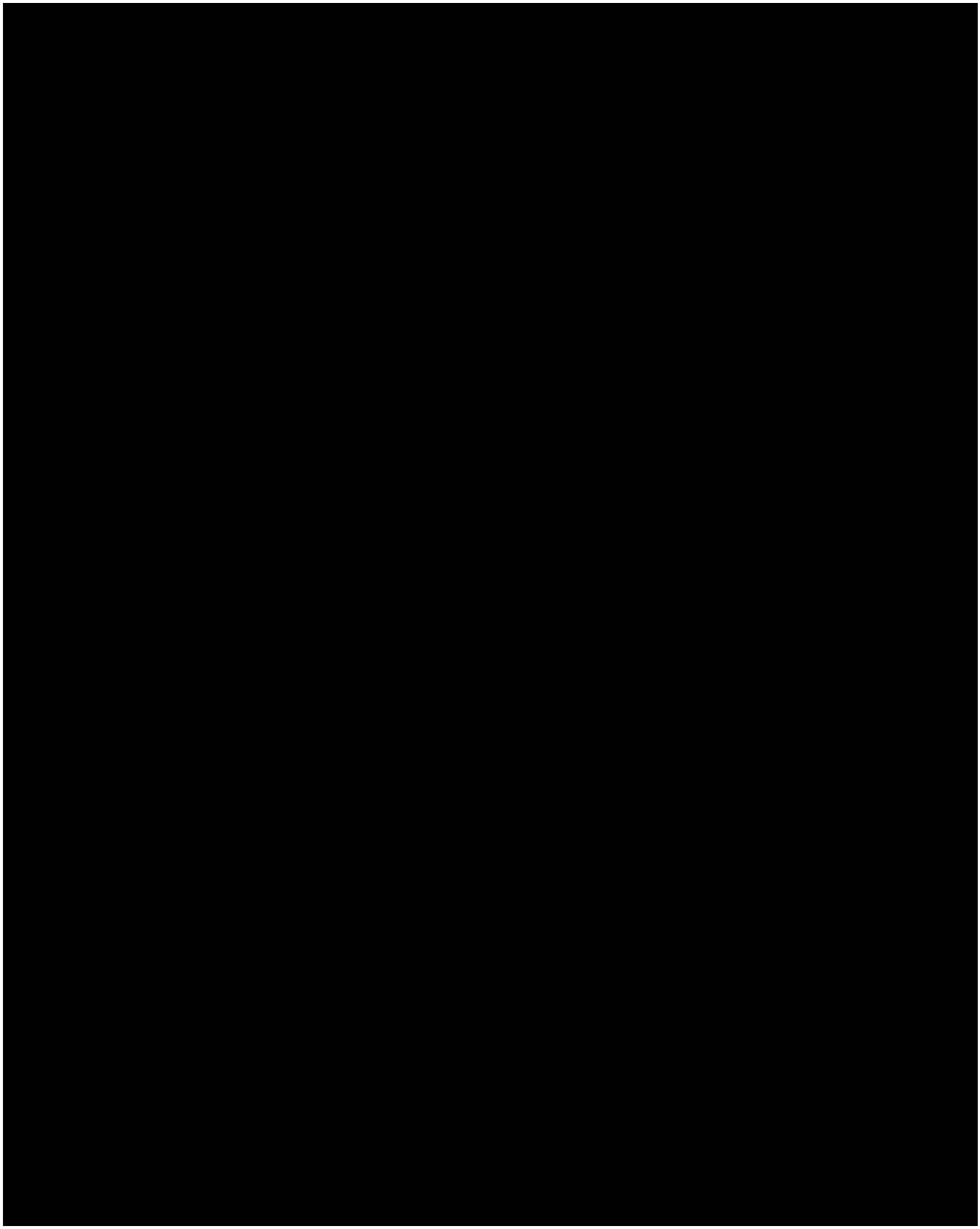


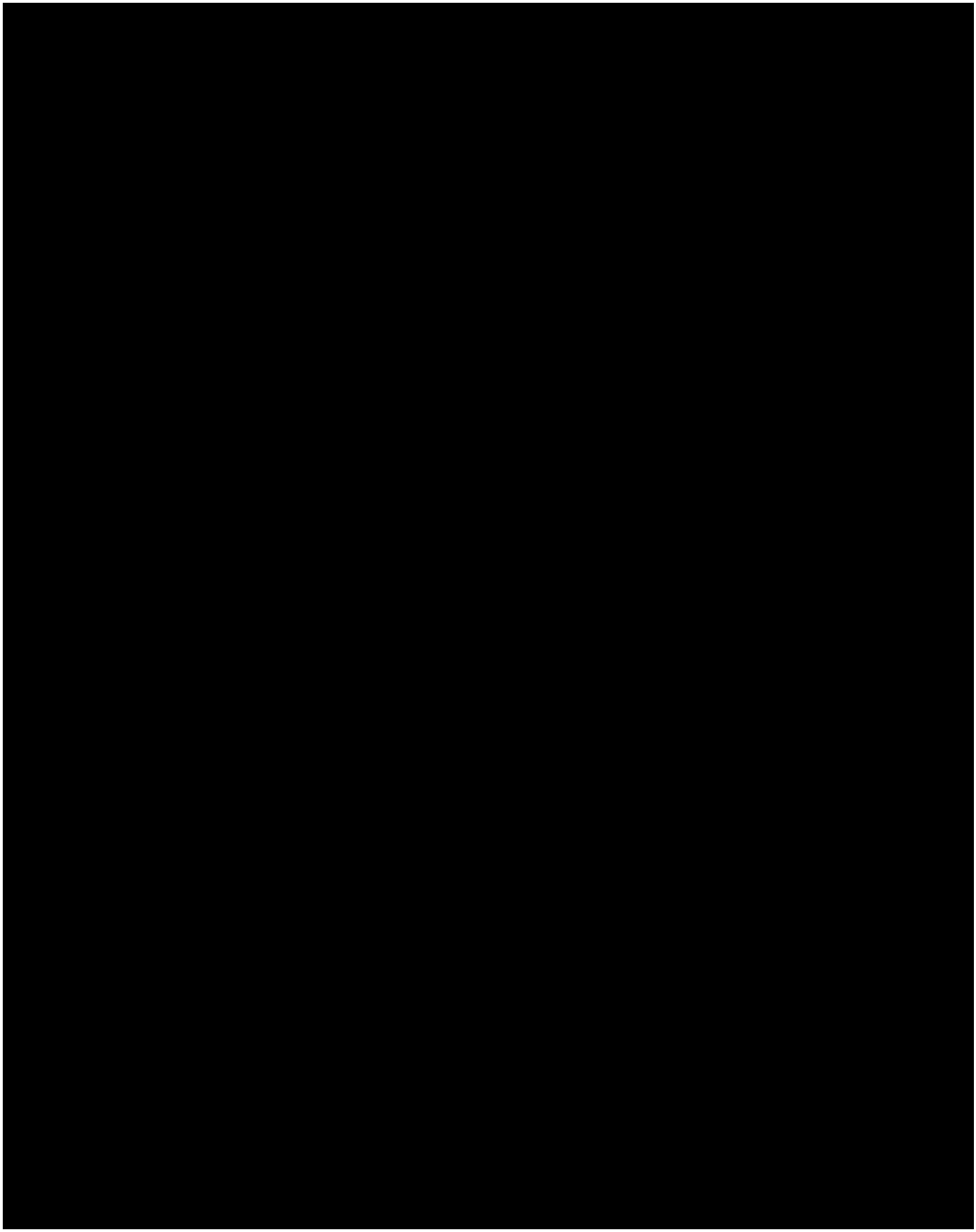


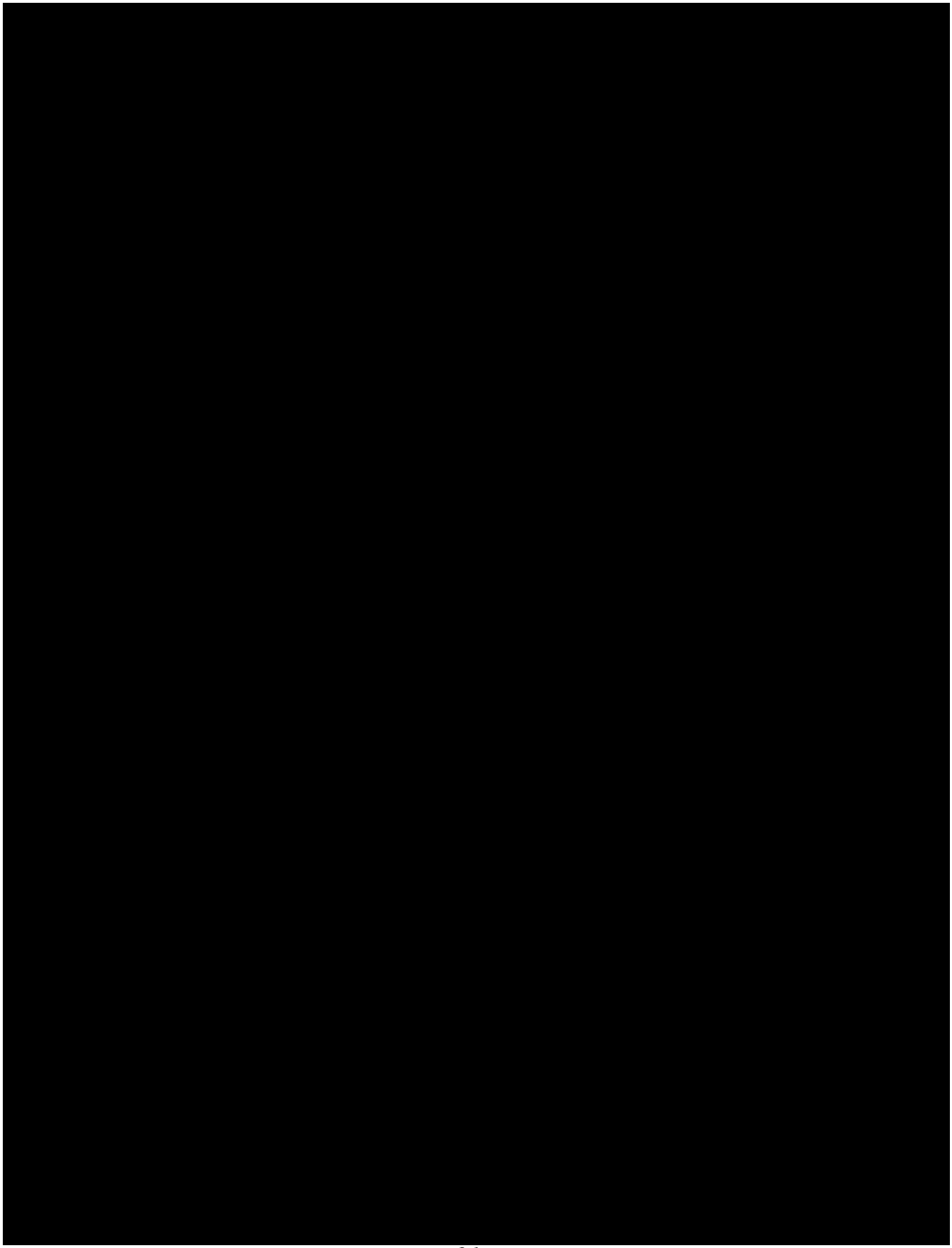


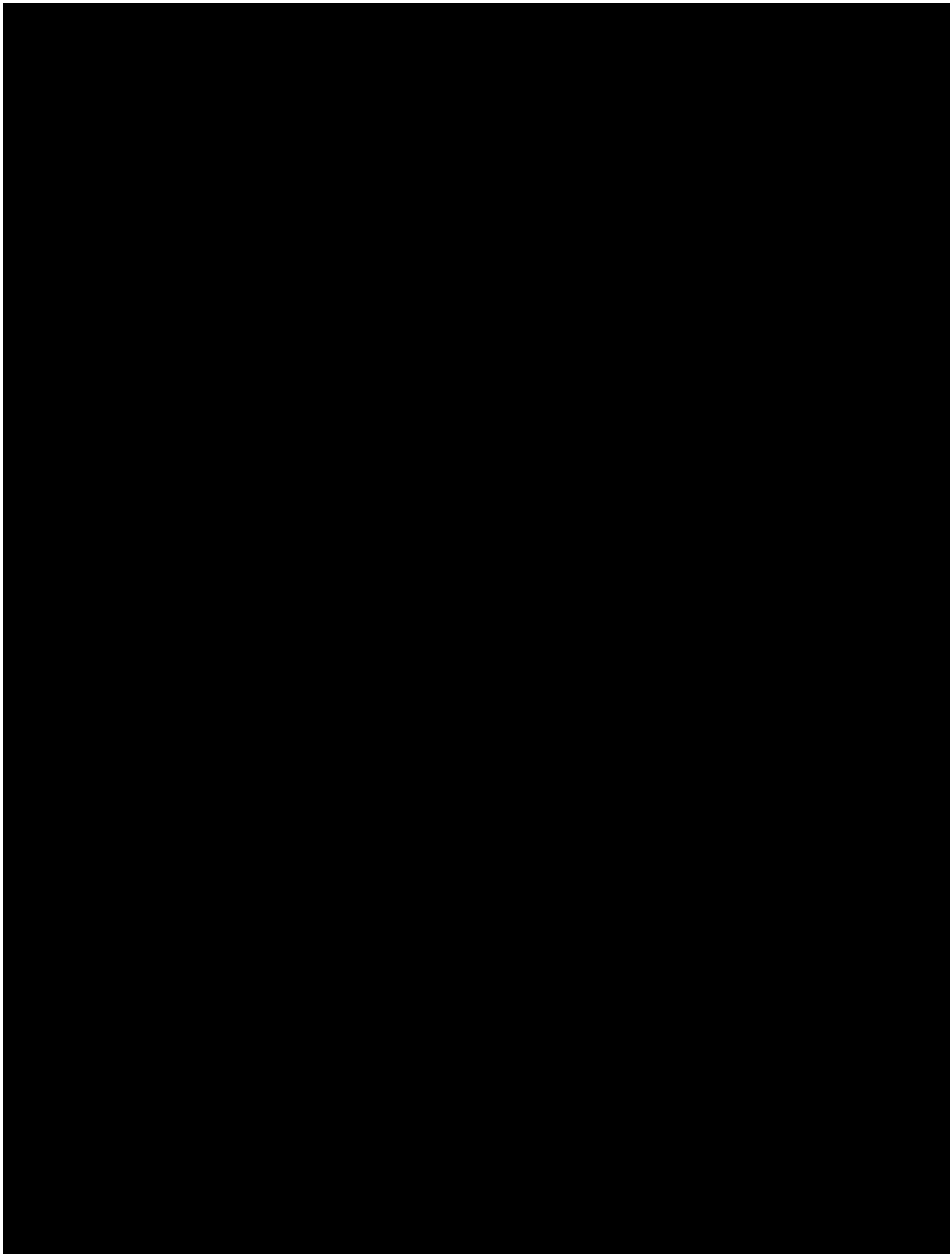


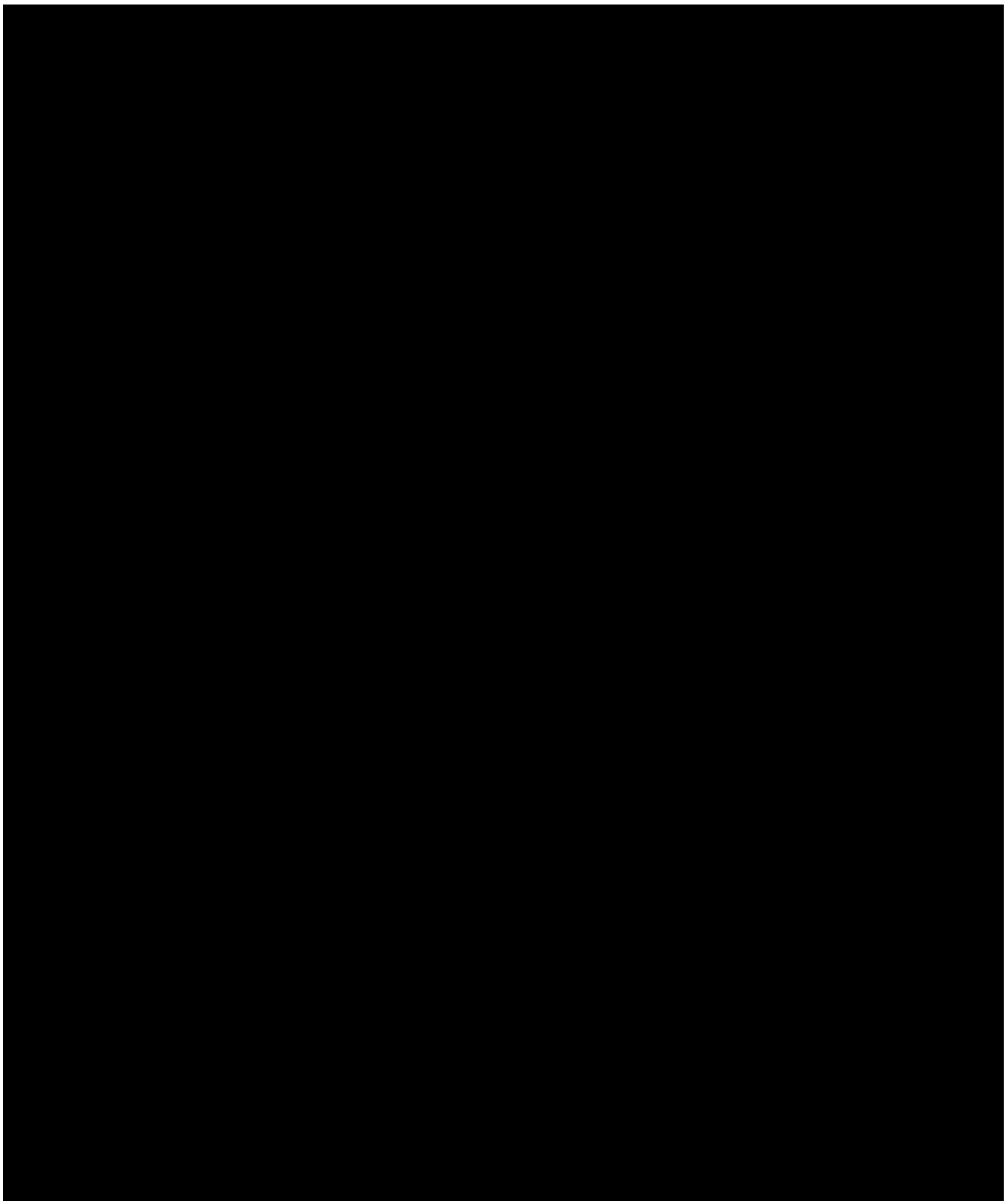


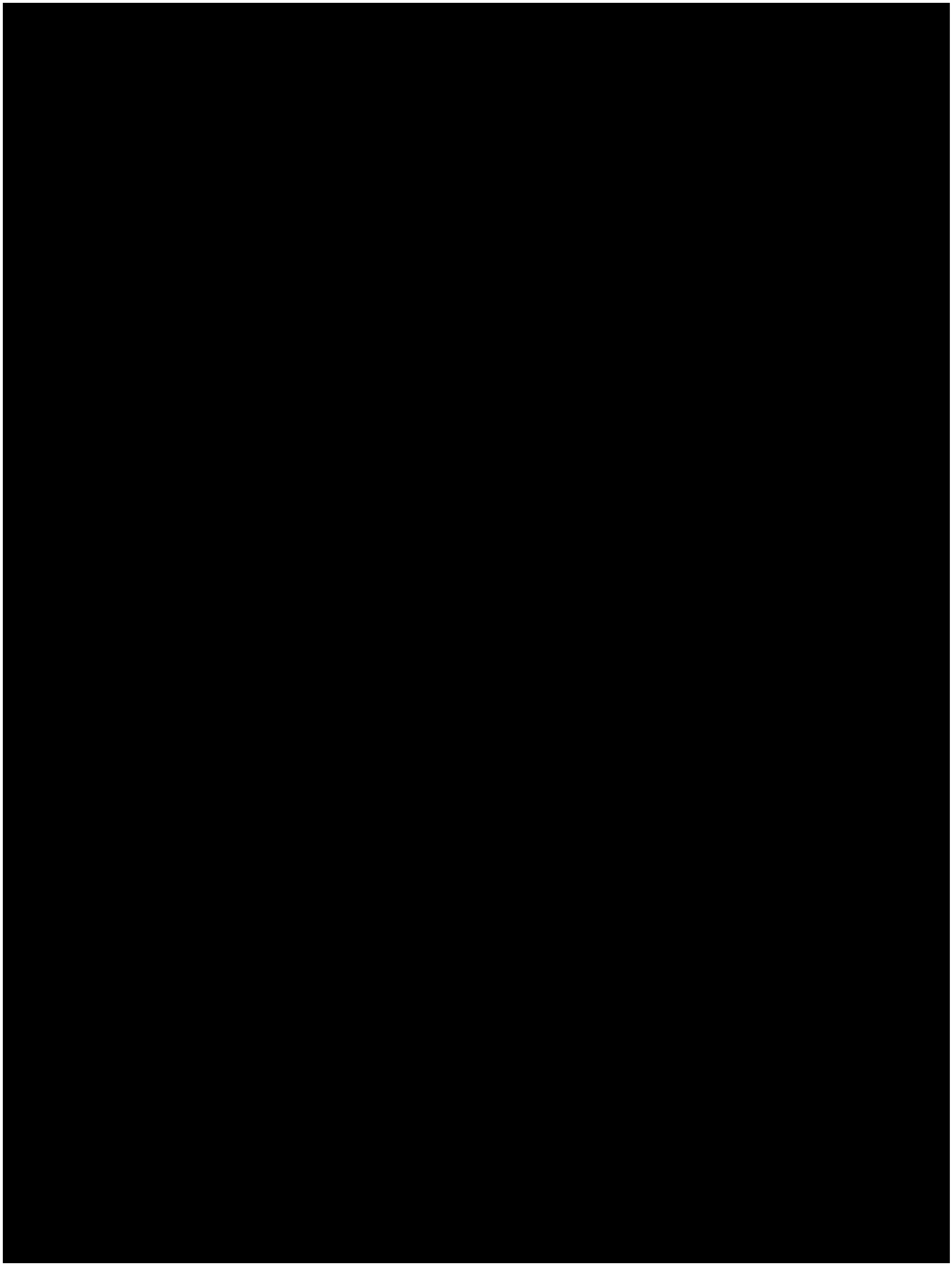


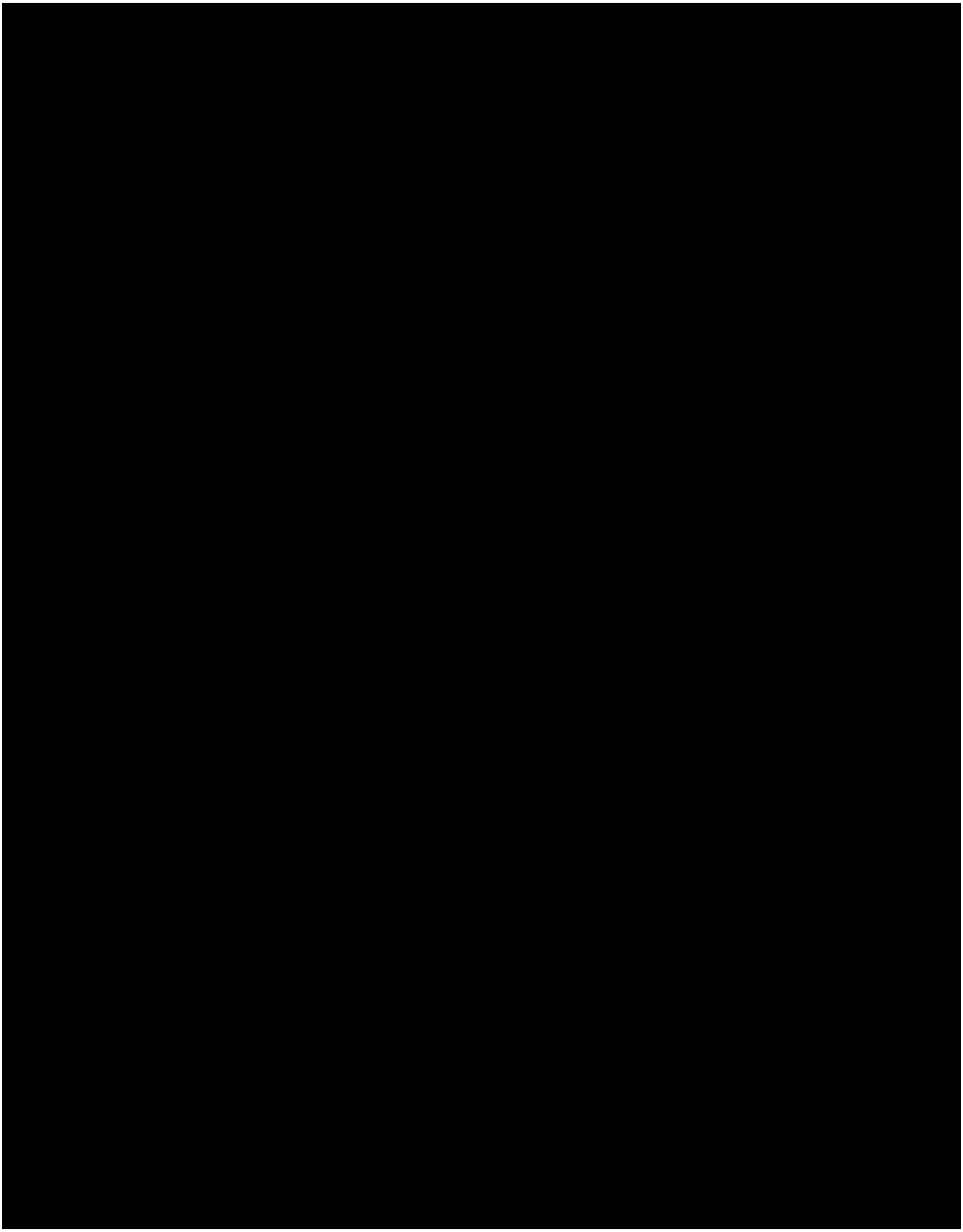


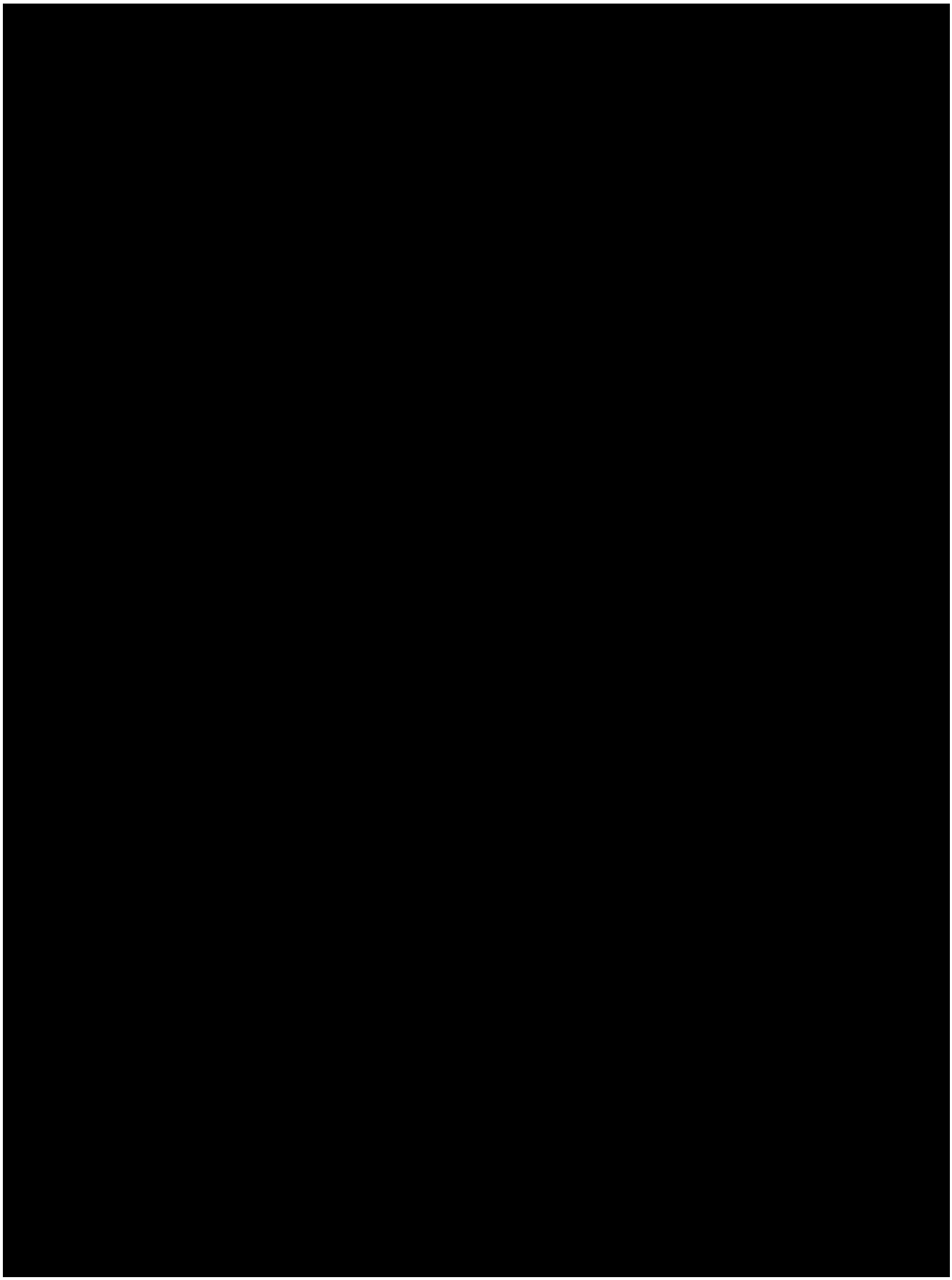


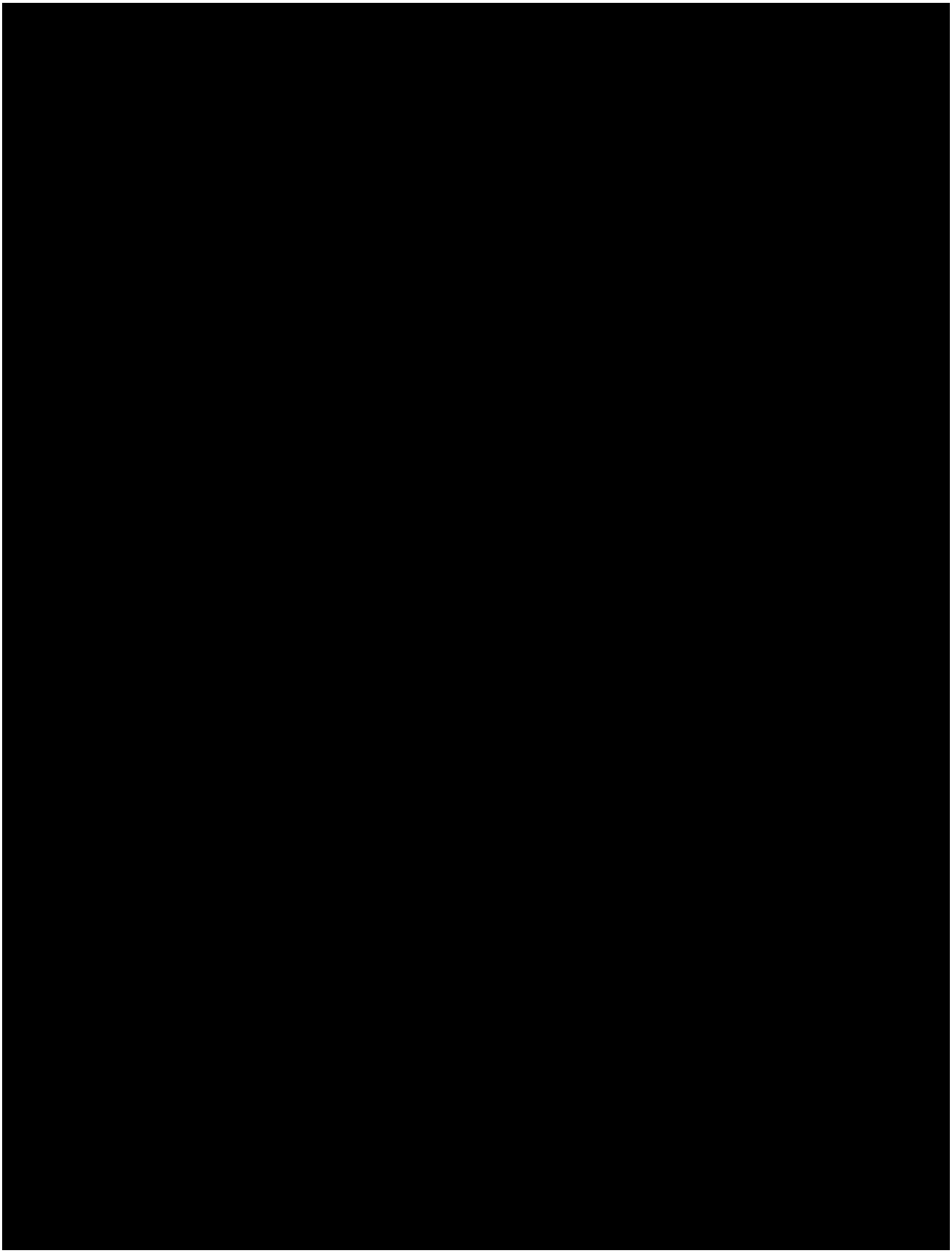


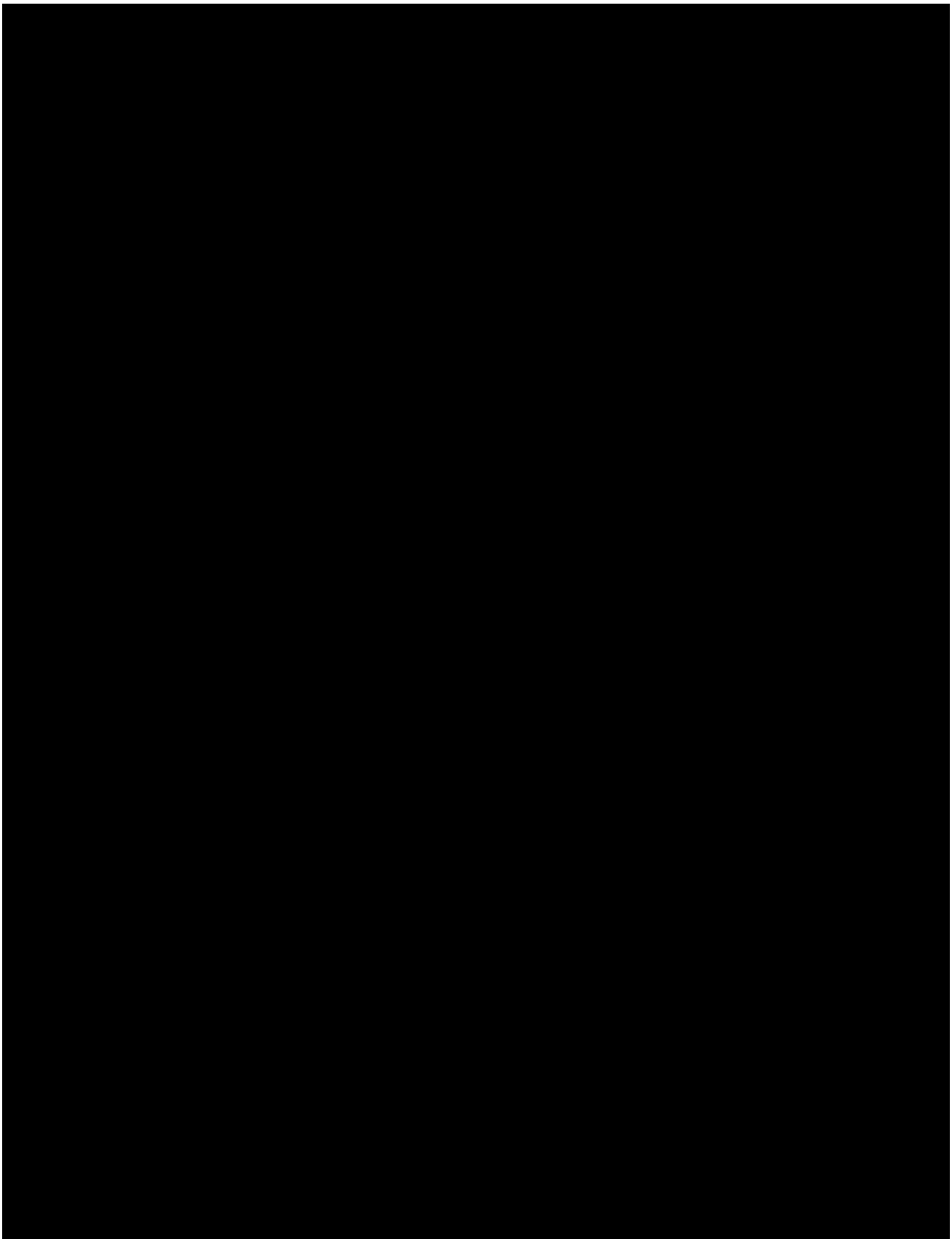


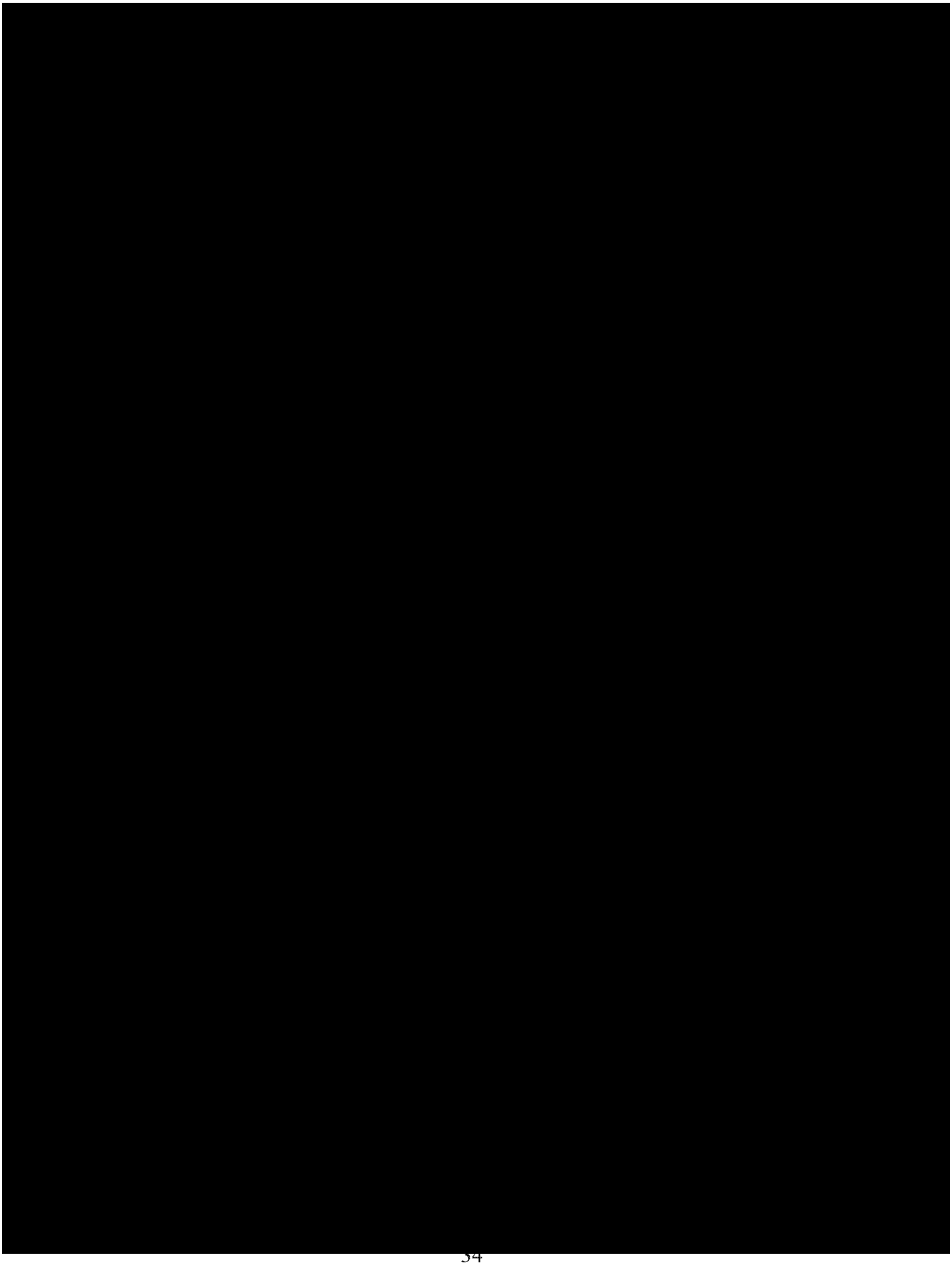


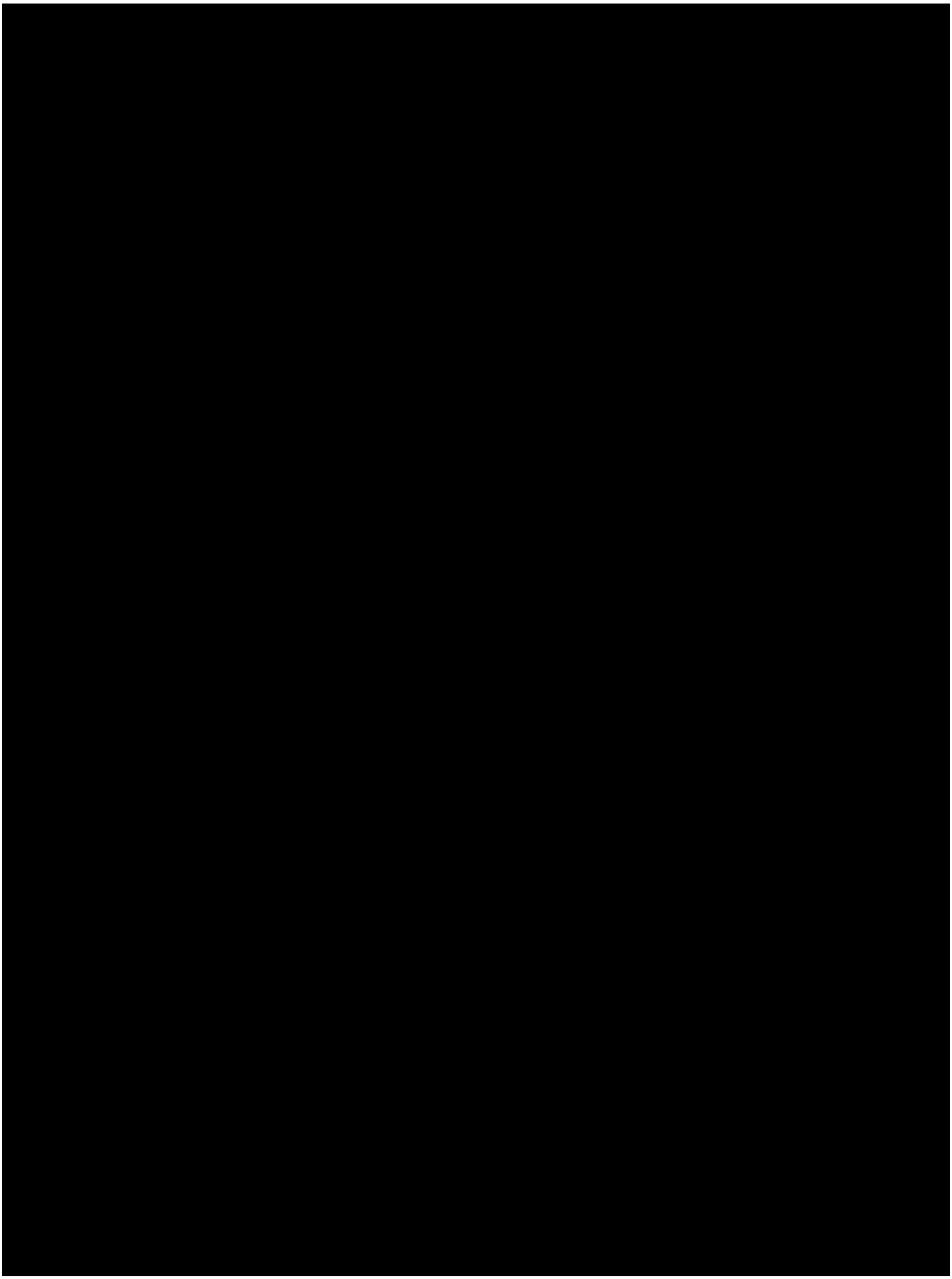


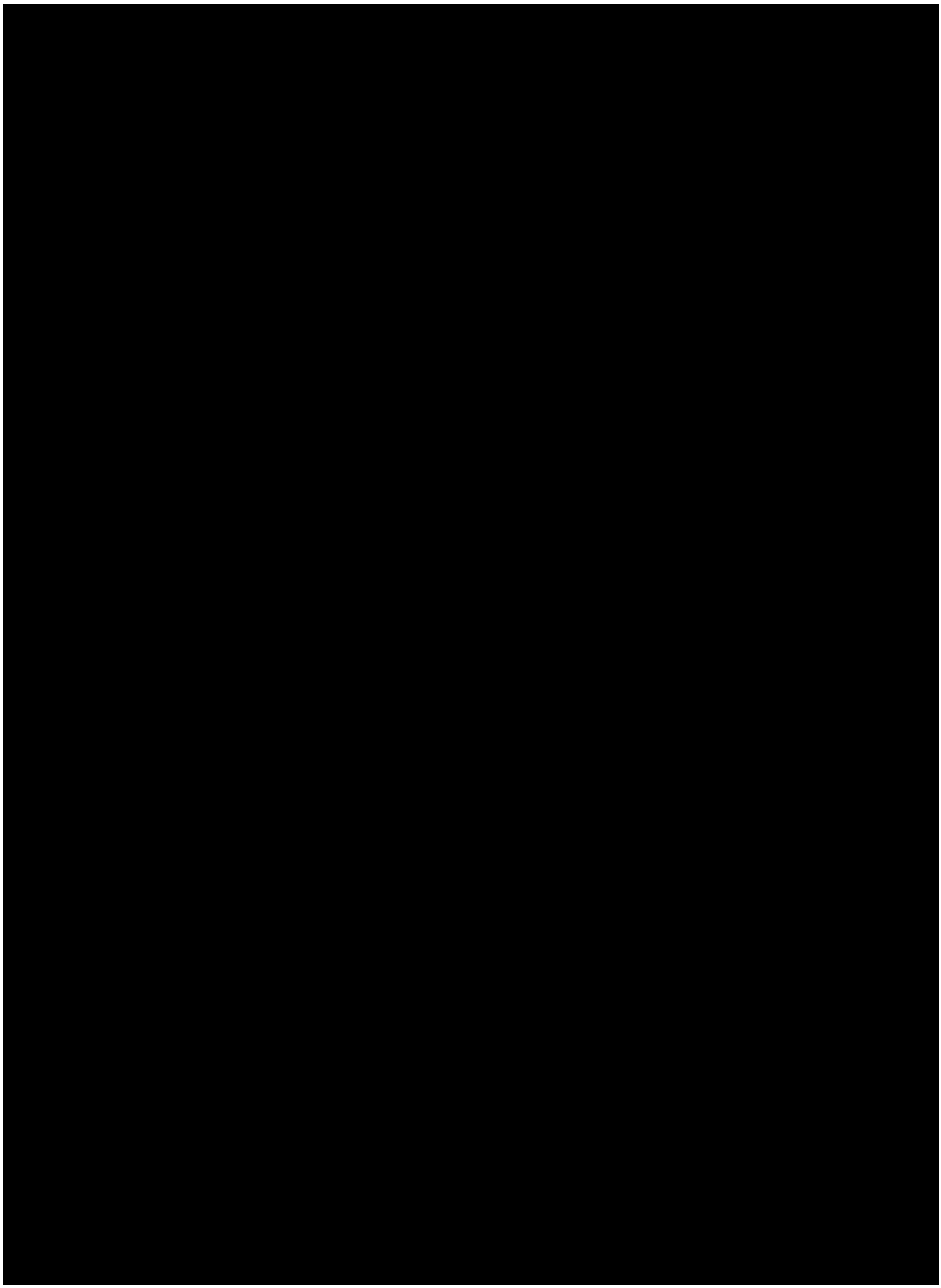


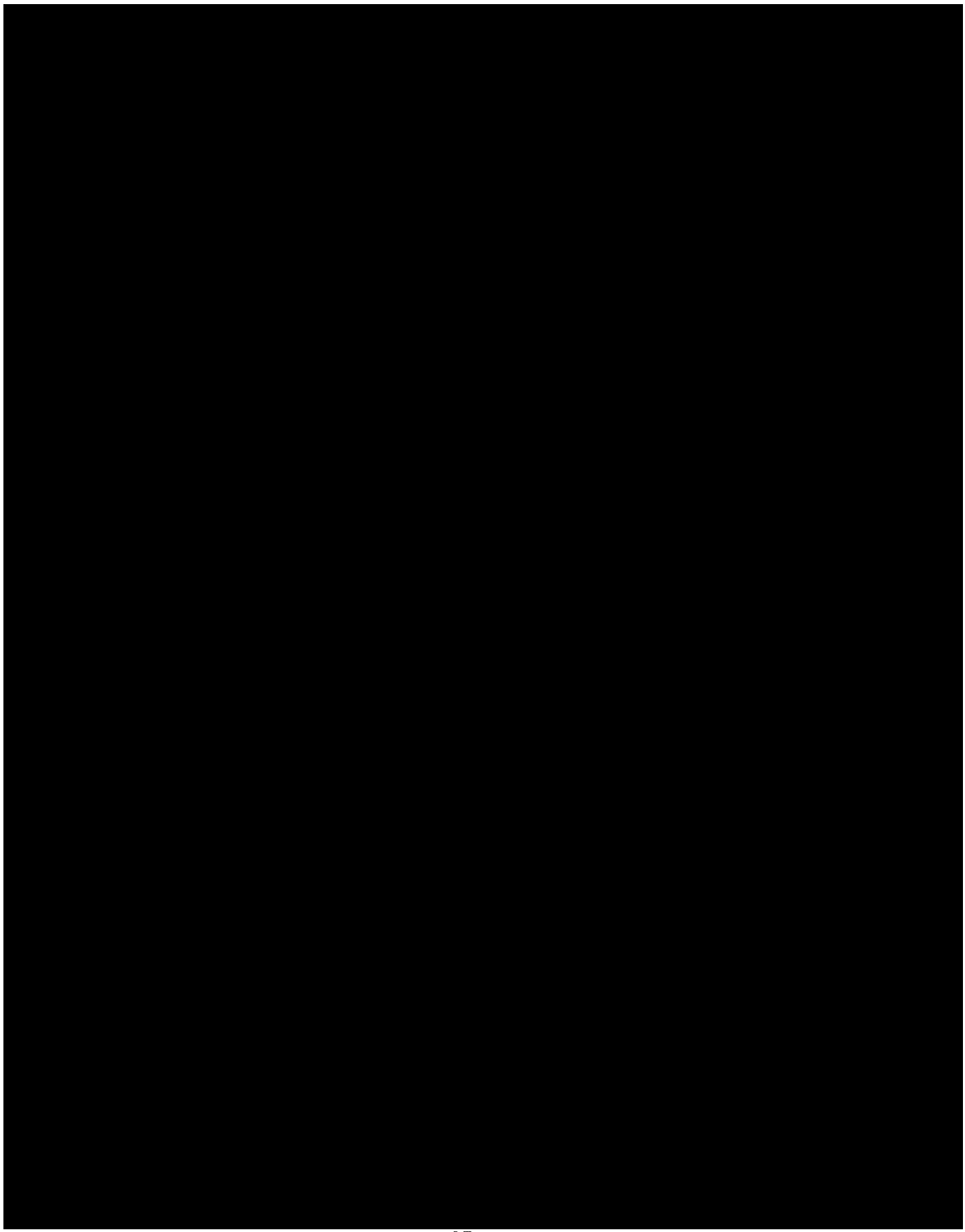


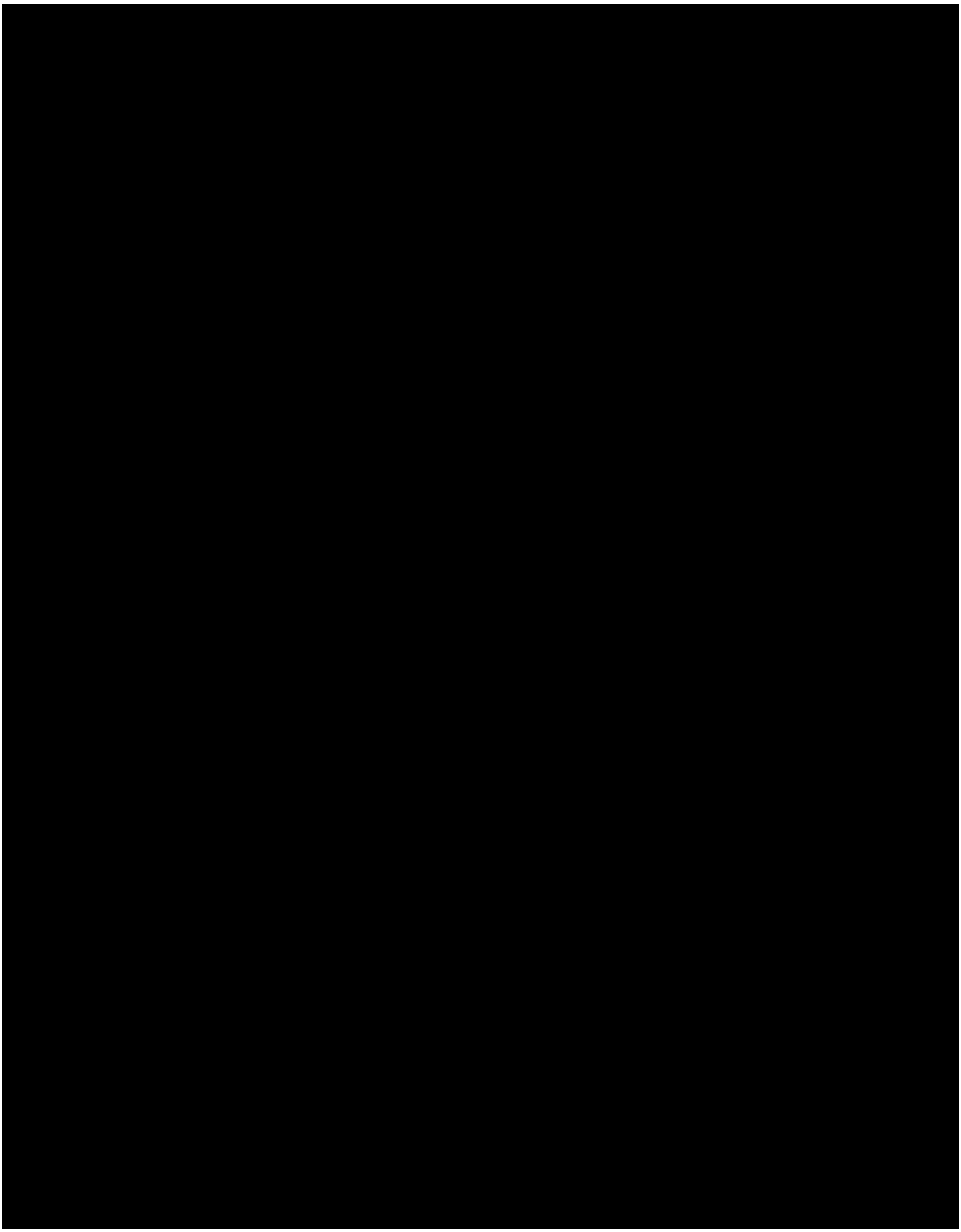


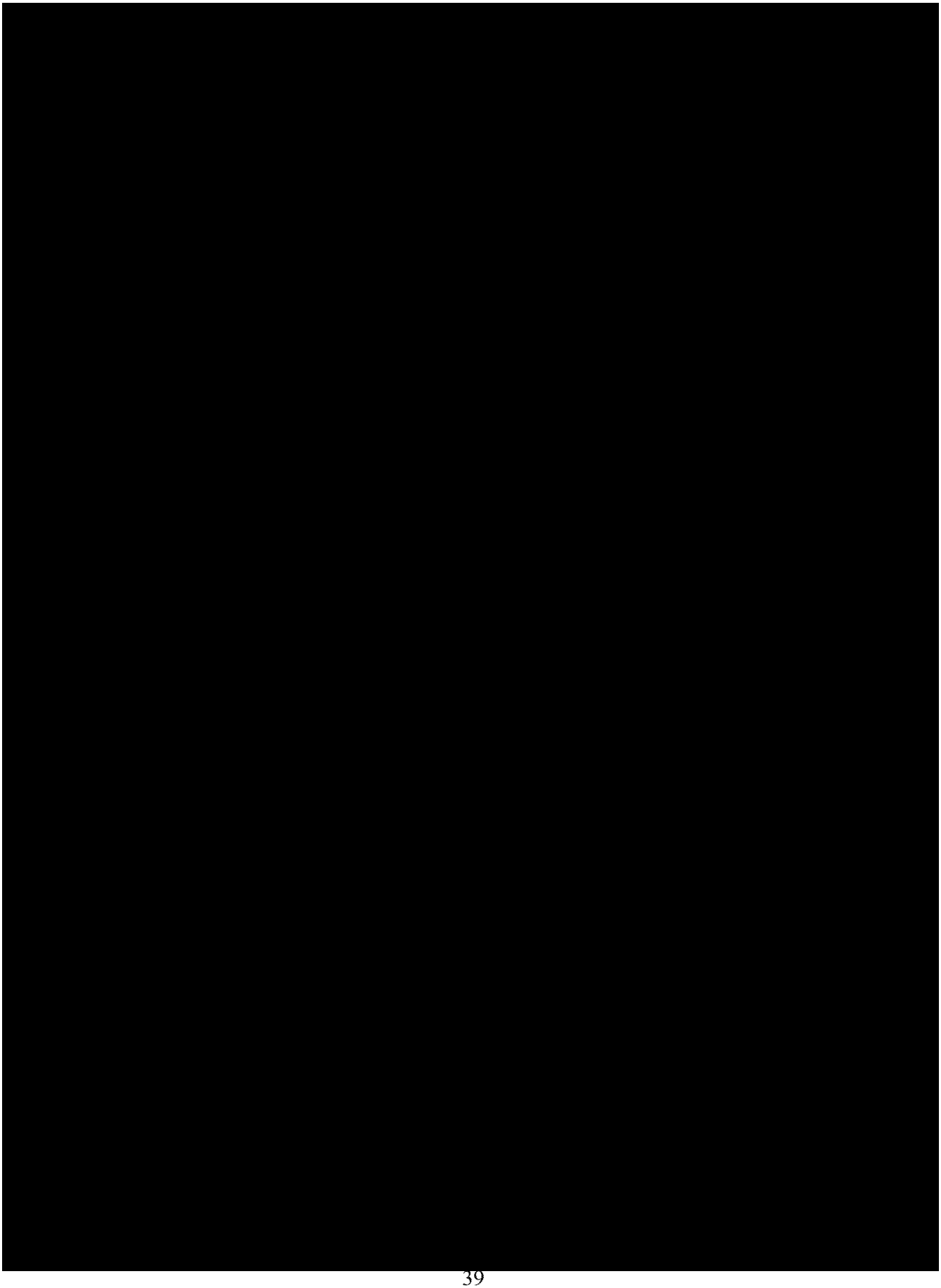


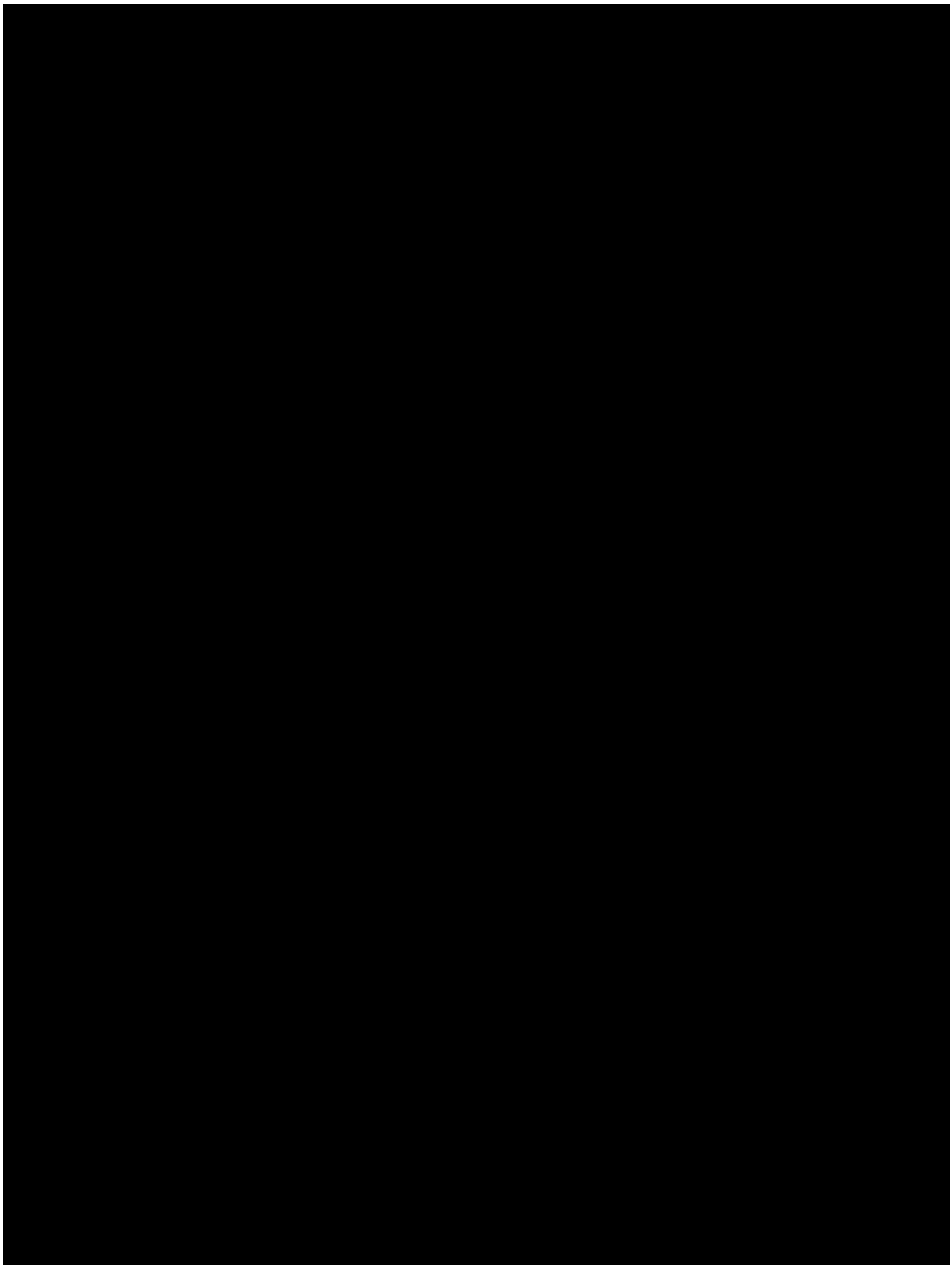


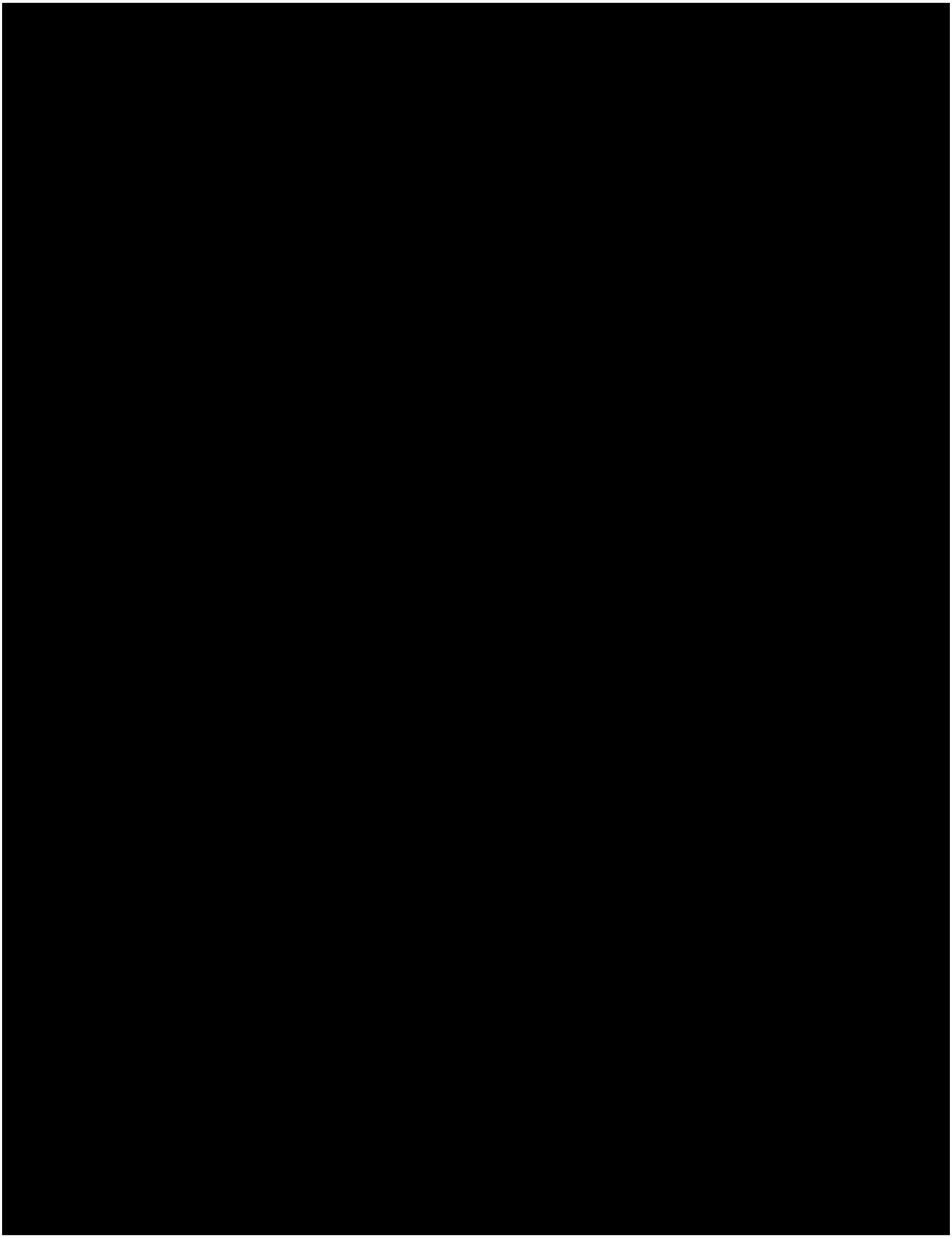


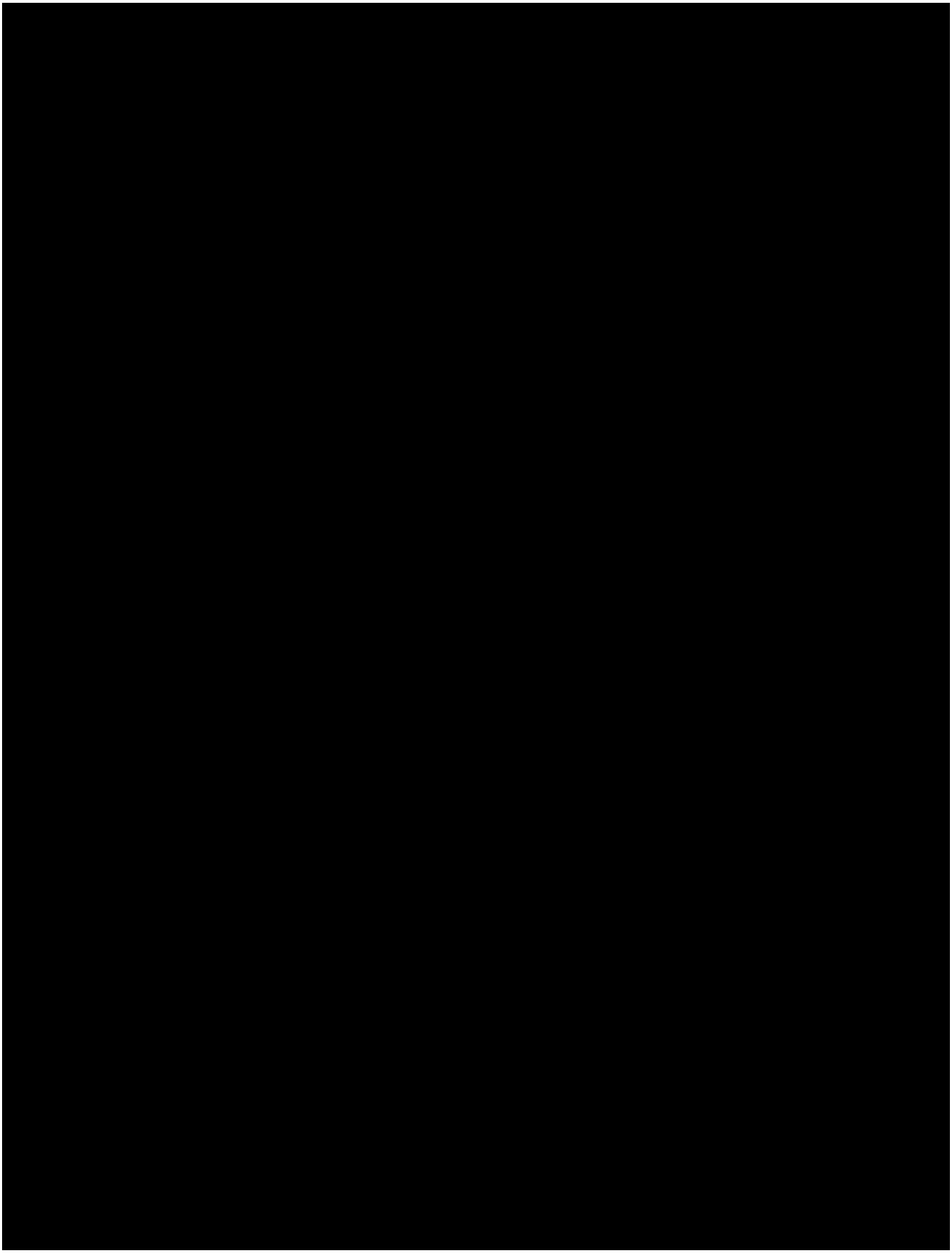


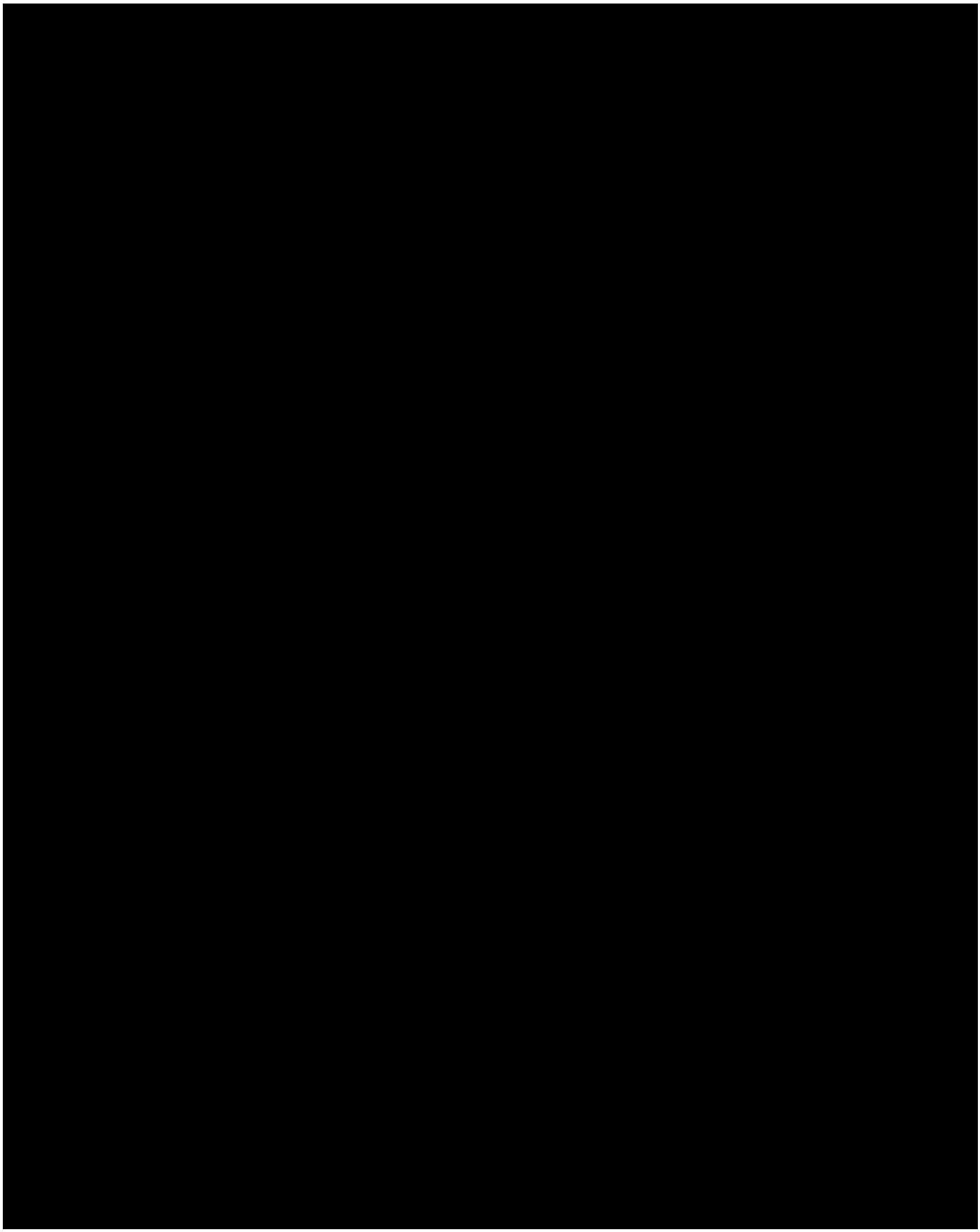


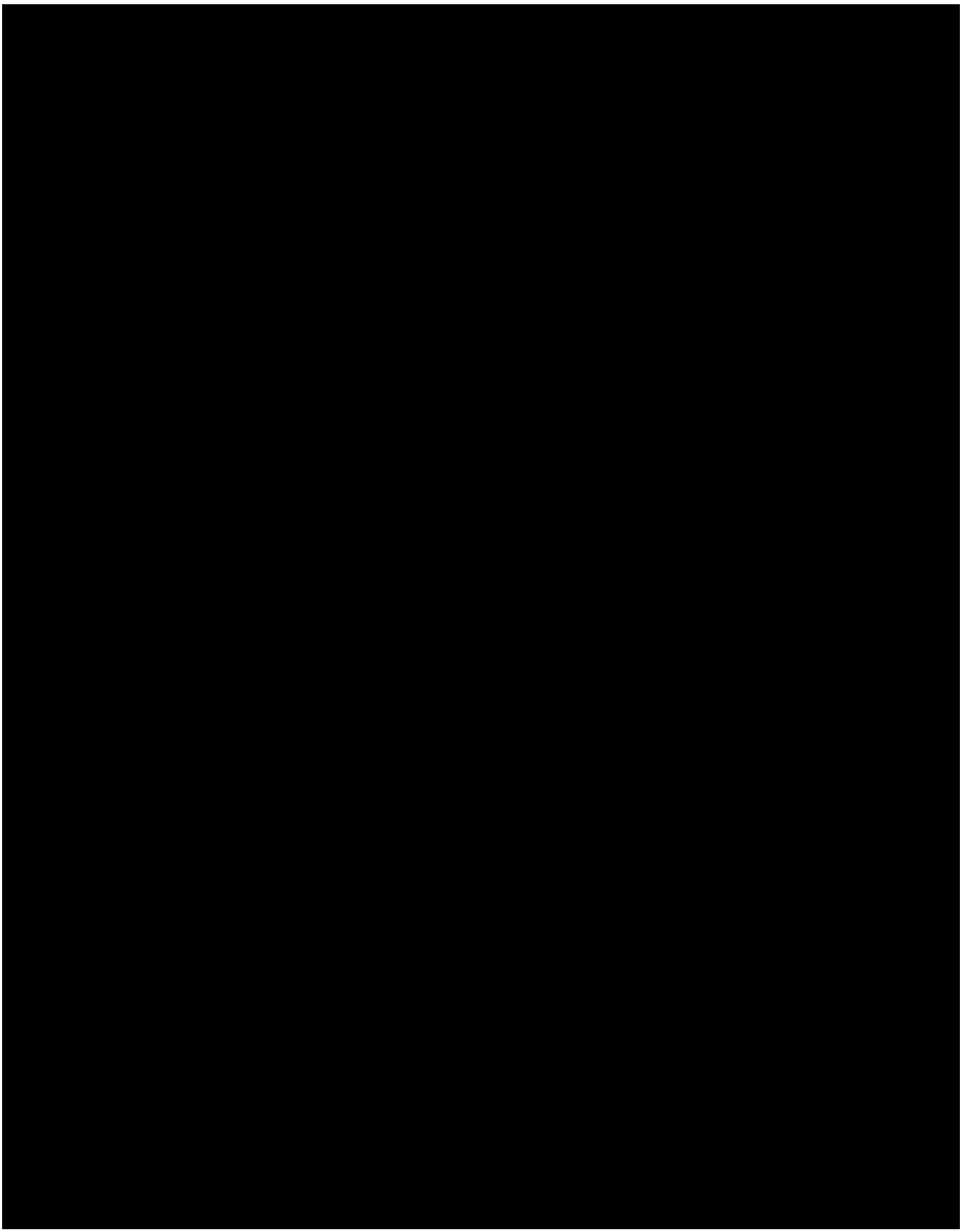


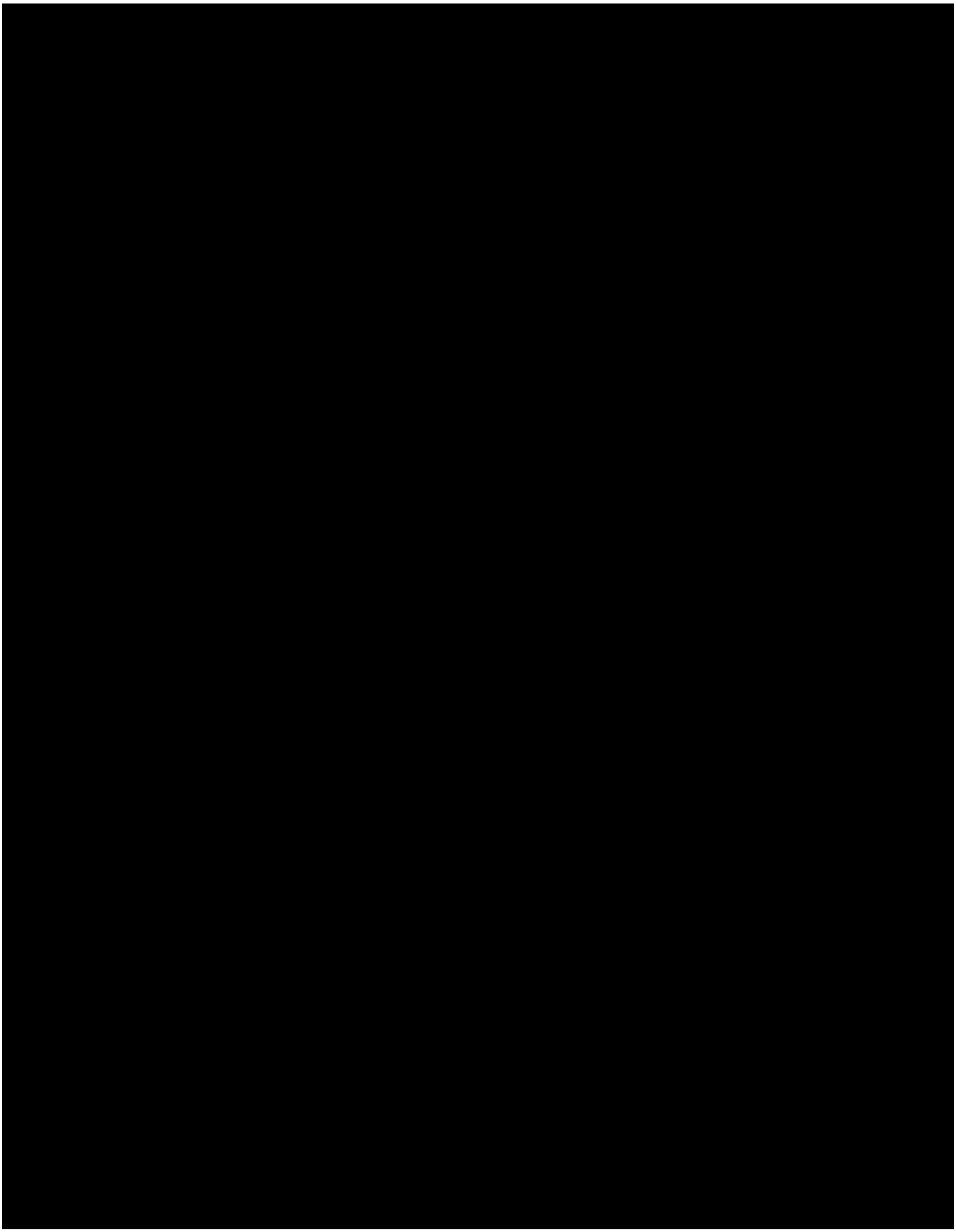


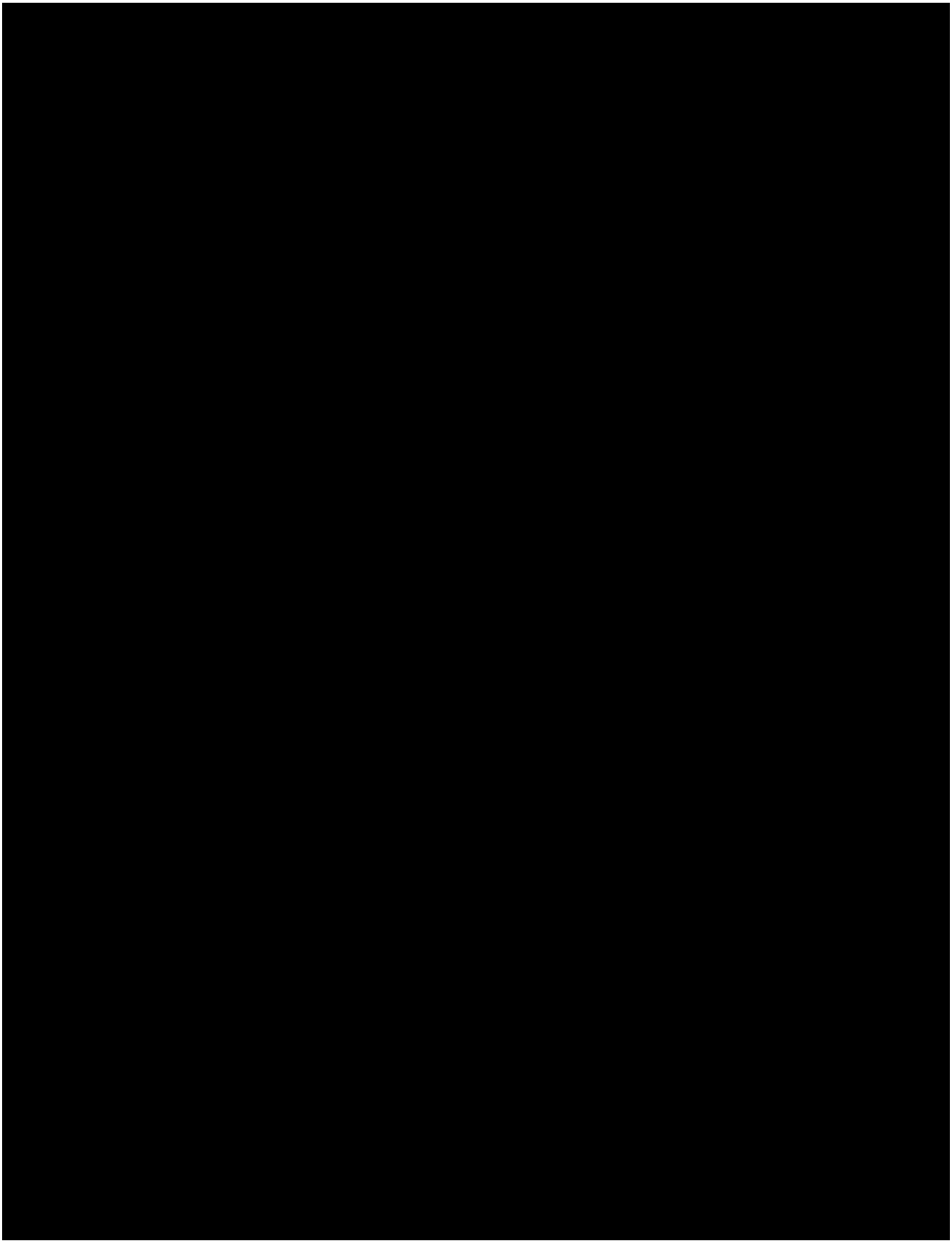


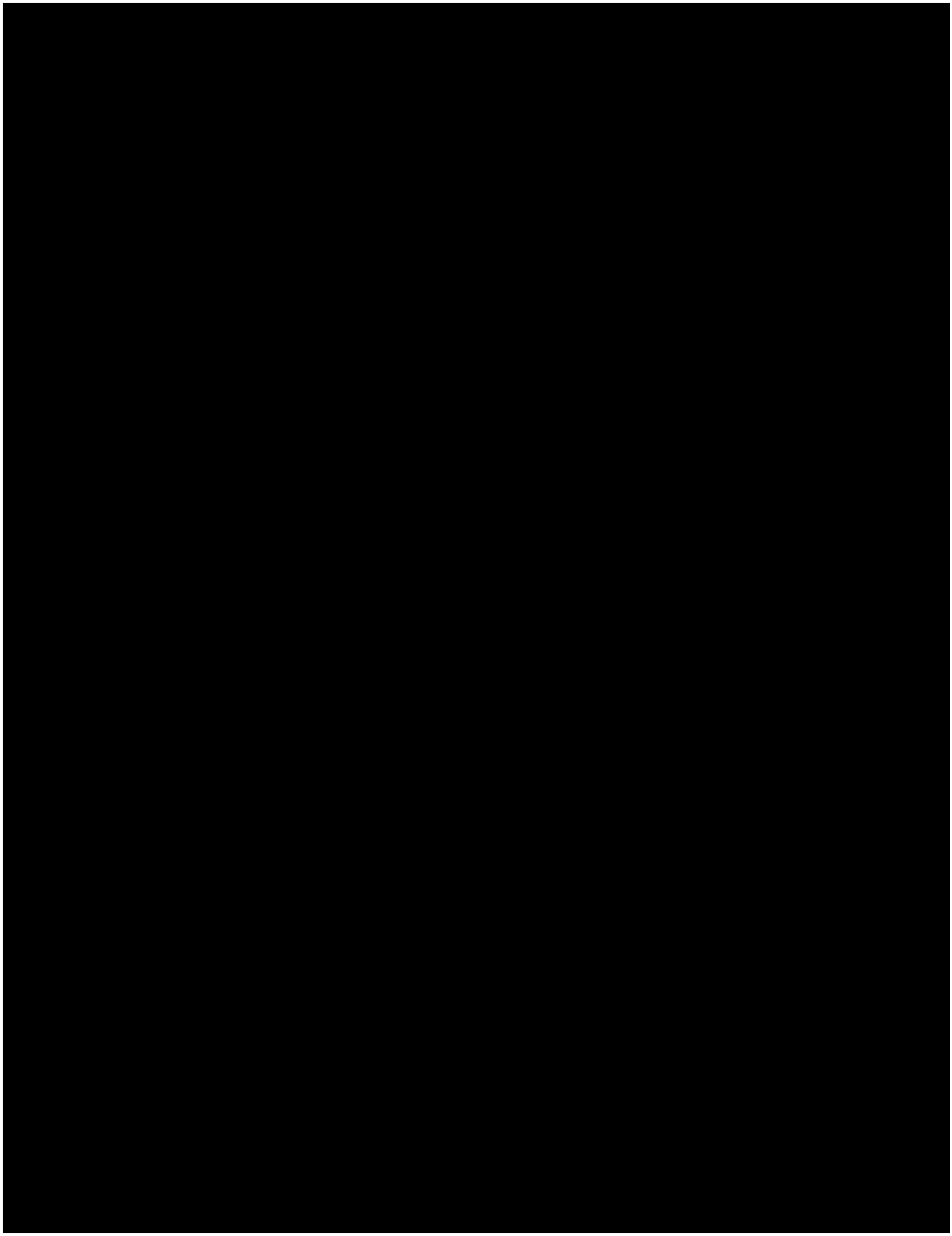


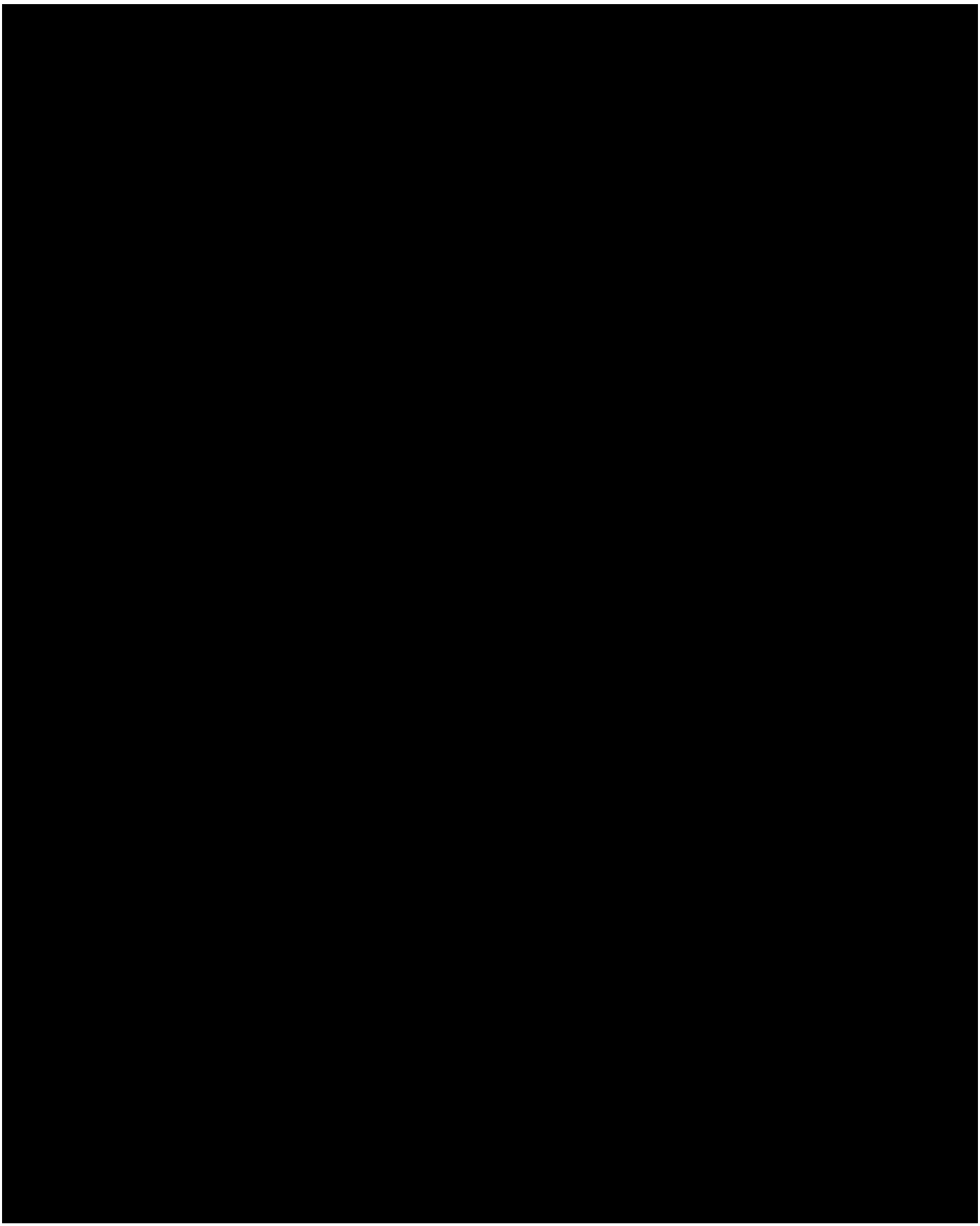












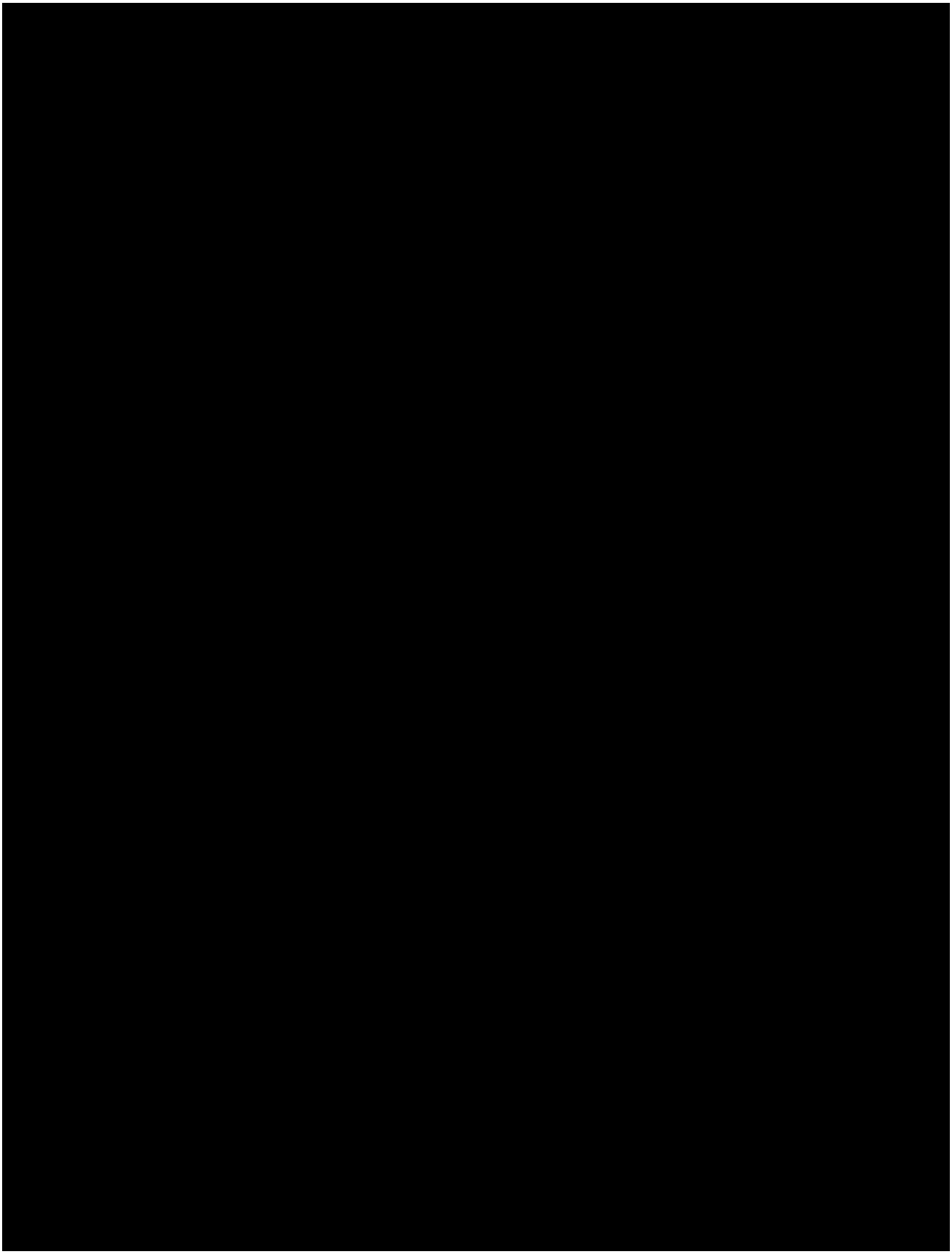


EXHIBIT A

ATTACHMENT C

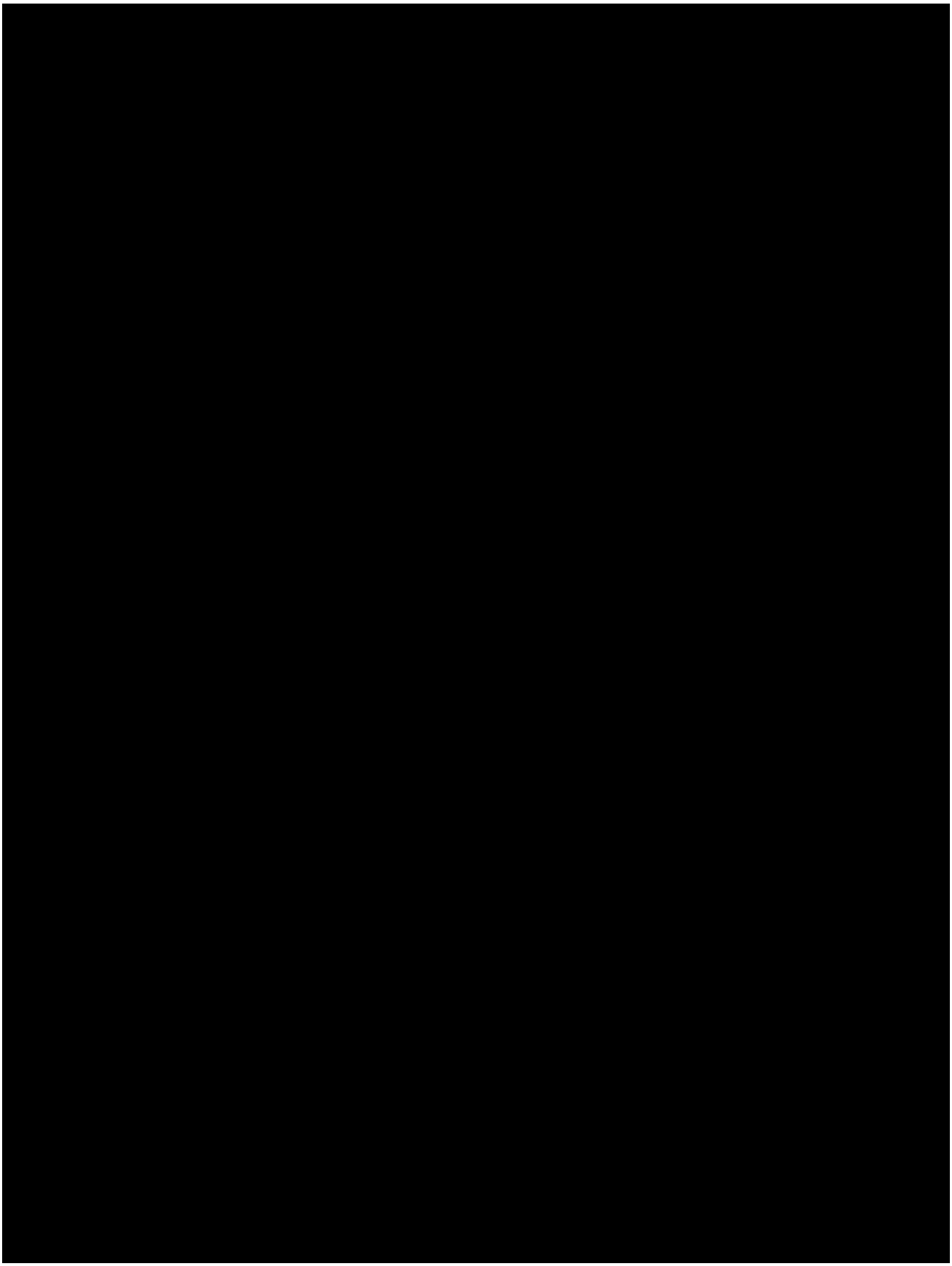
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

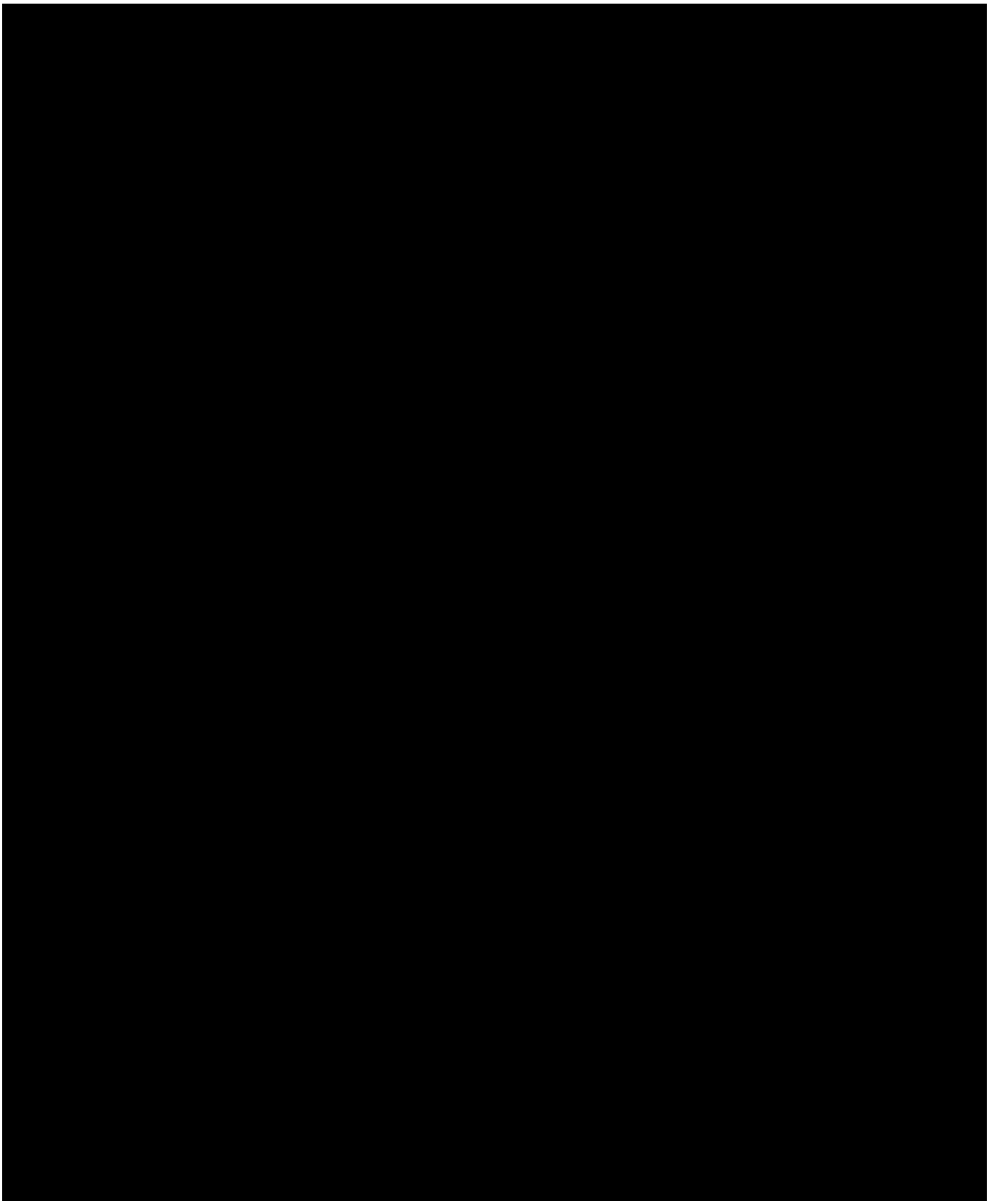
IN THE MATTER OF THE SEARCH OF ALL ELECTRONIC DEVICES ON THE PERSON OF WAEL HANA [redacted]	:	**TO BE FILED UNDER SEAL** Hon. Leda Dunn Wettre Mag. No. 19-8415 Mag. No. 19-8416 Mag. No. 19-8417 Mag. No. 19-8418 **AFFIDAVIT**

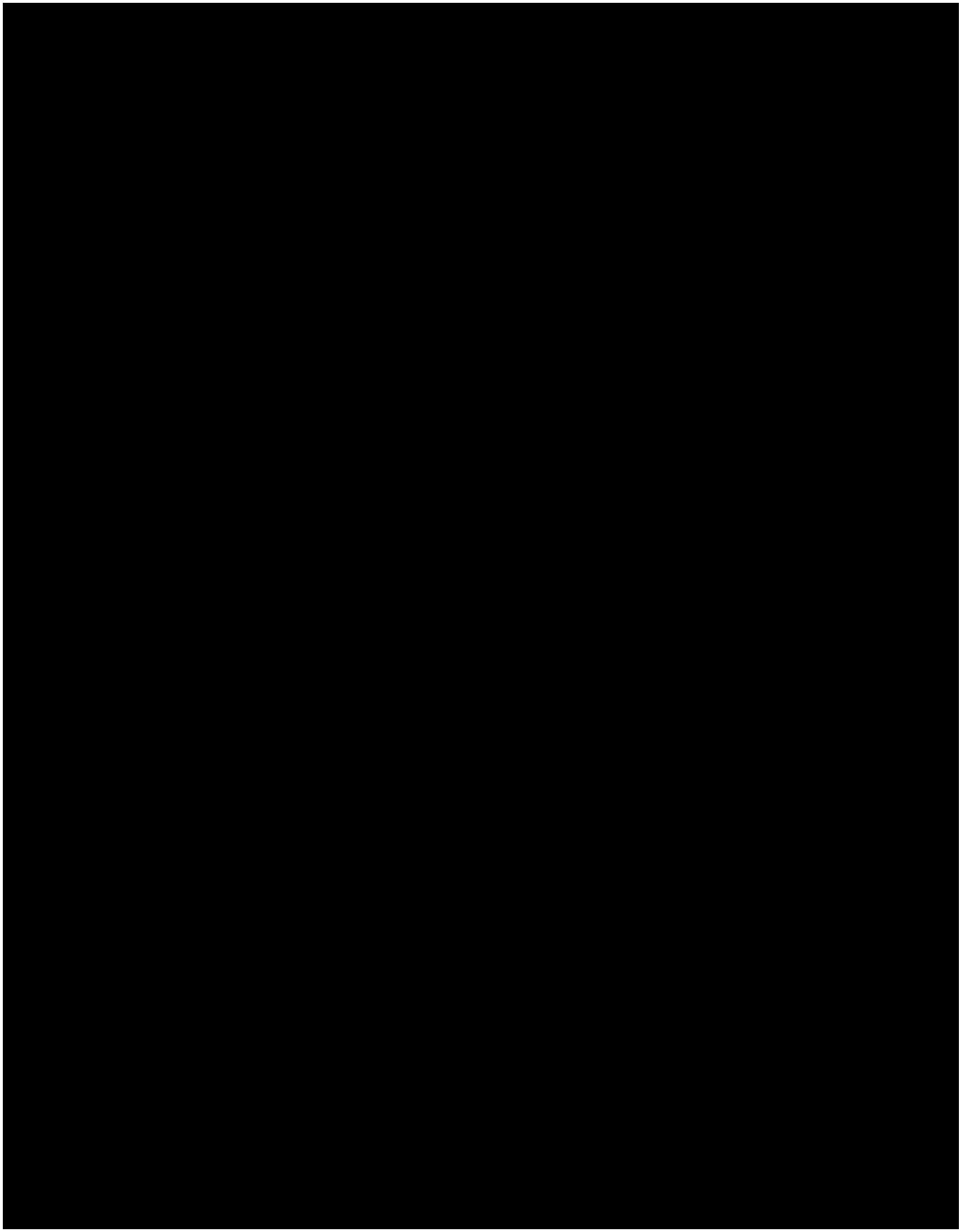
STATE OF NEW JERSEY :
ss.
COUNTY OF ESSEX :

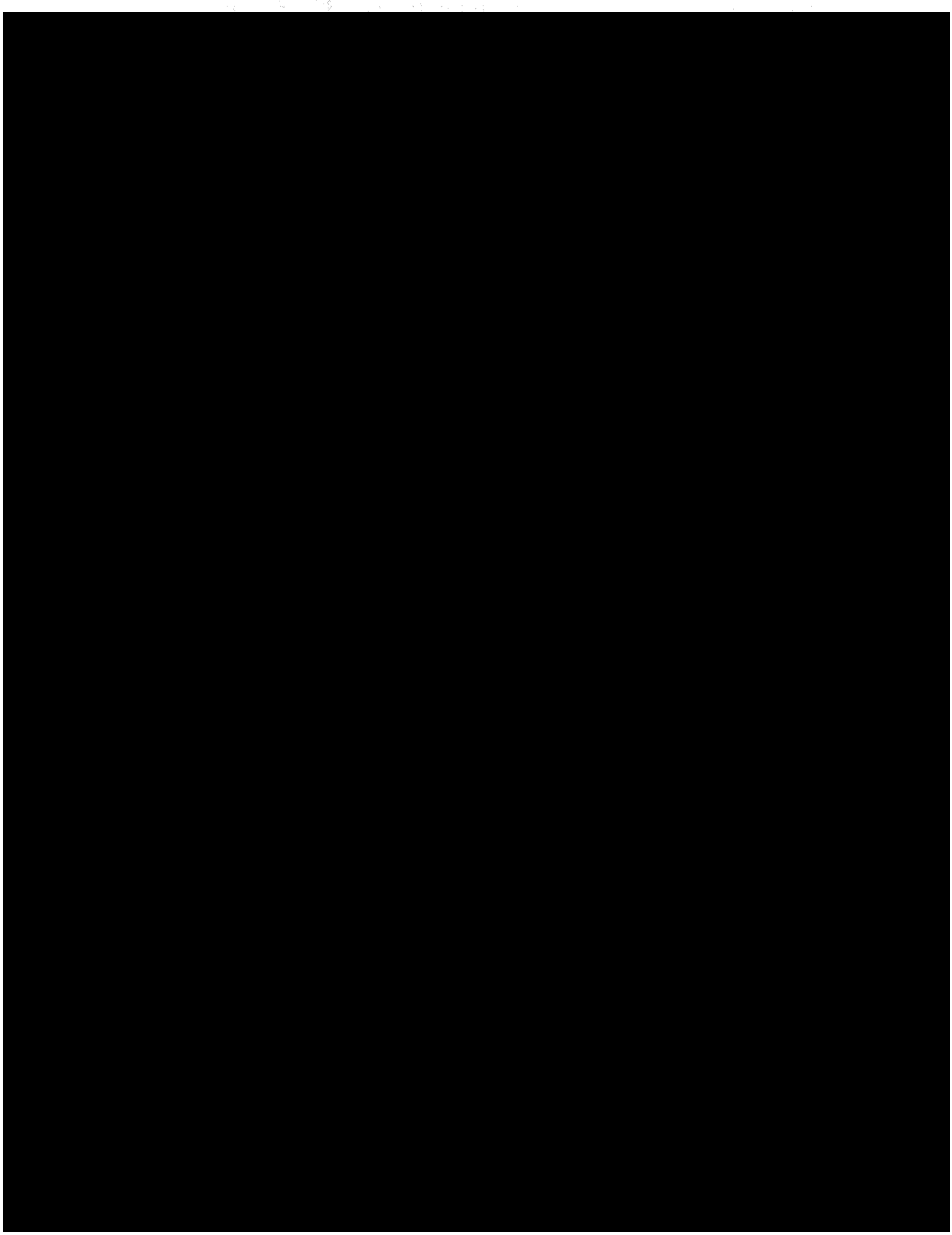
[redacted], being duly sworn, deposes and says:

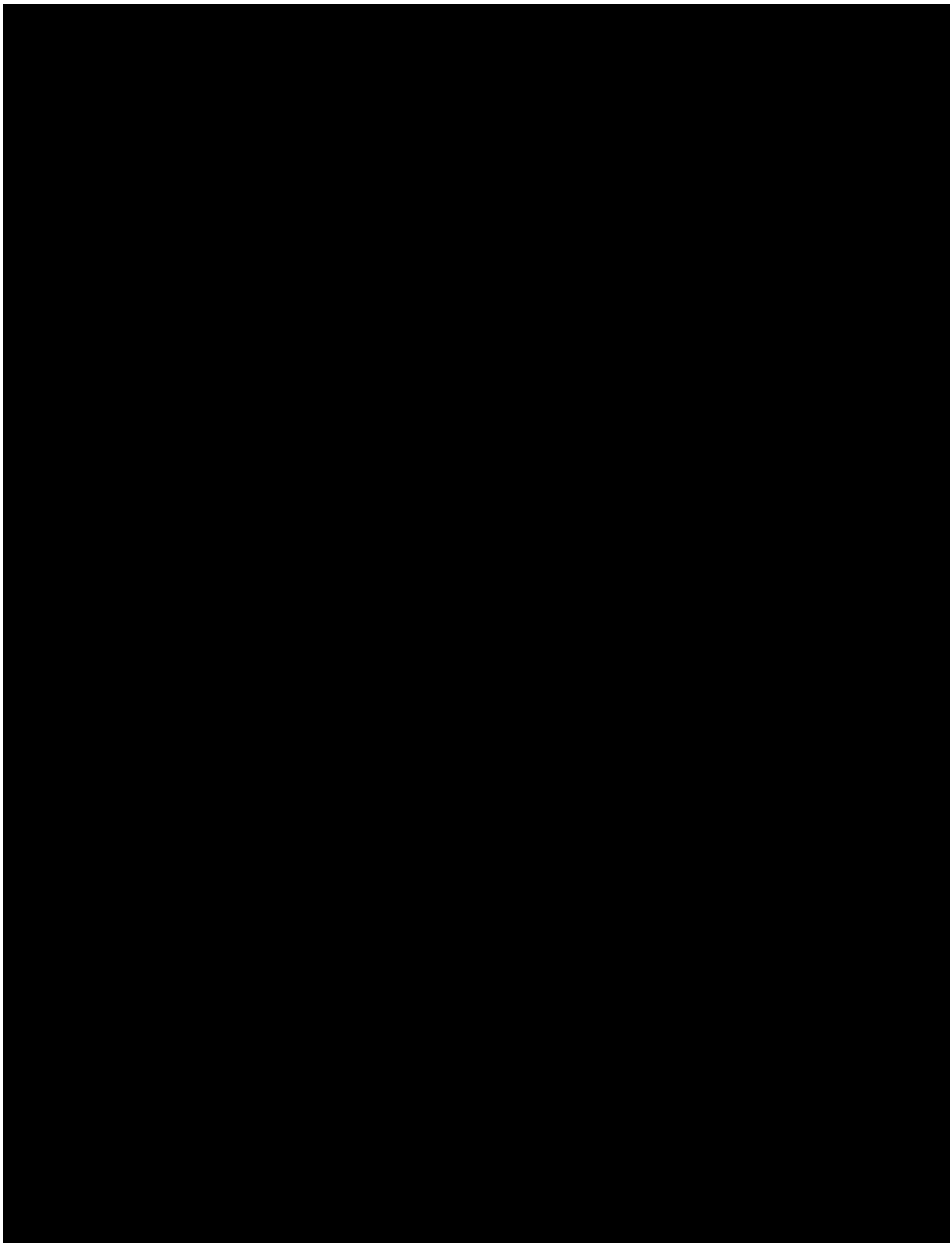
[redacted]

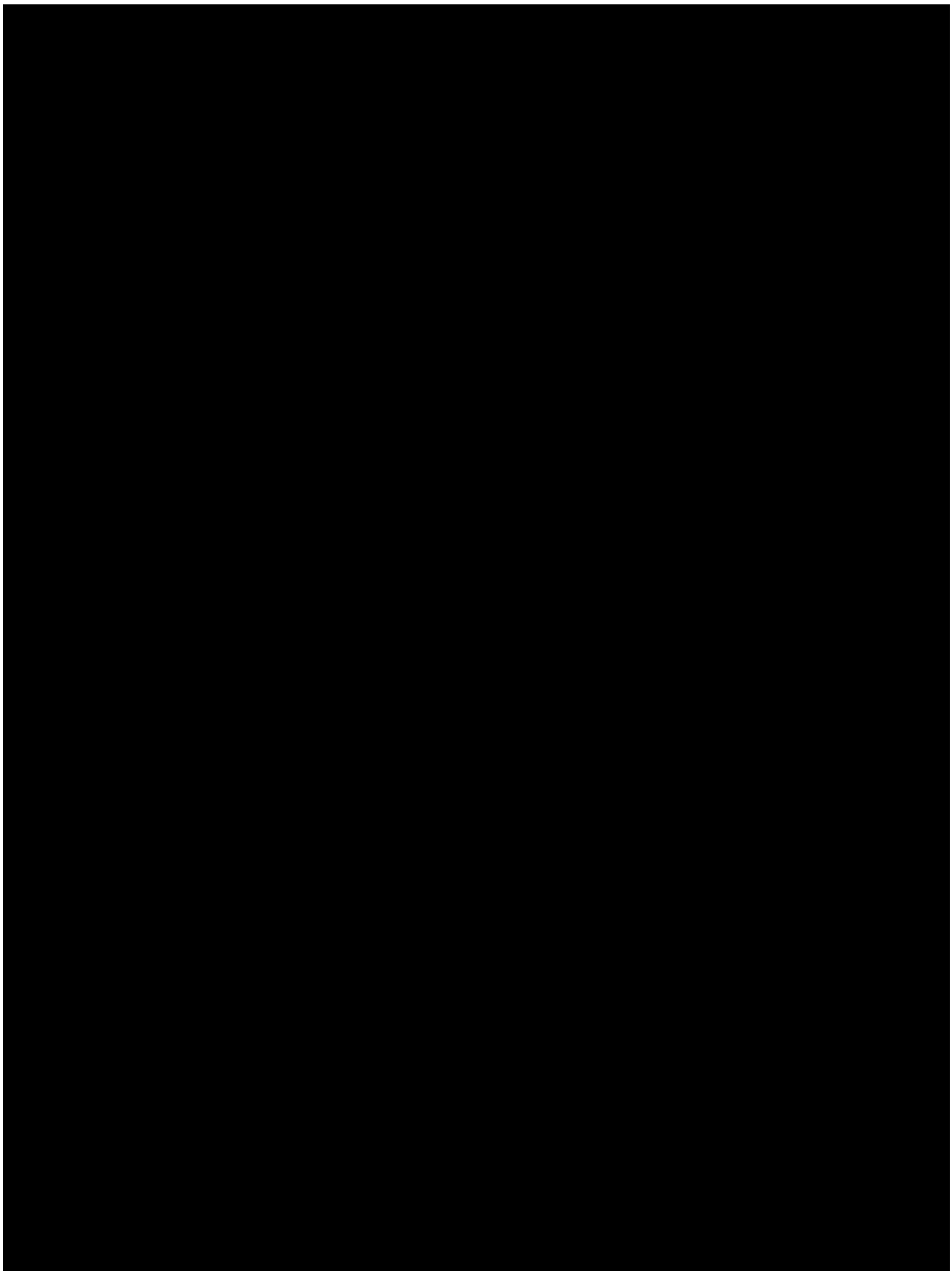


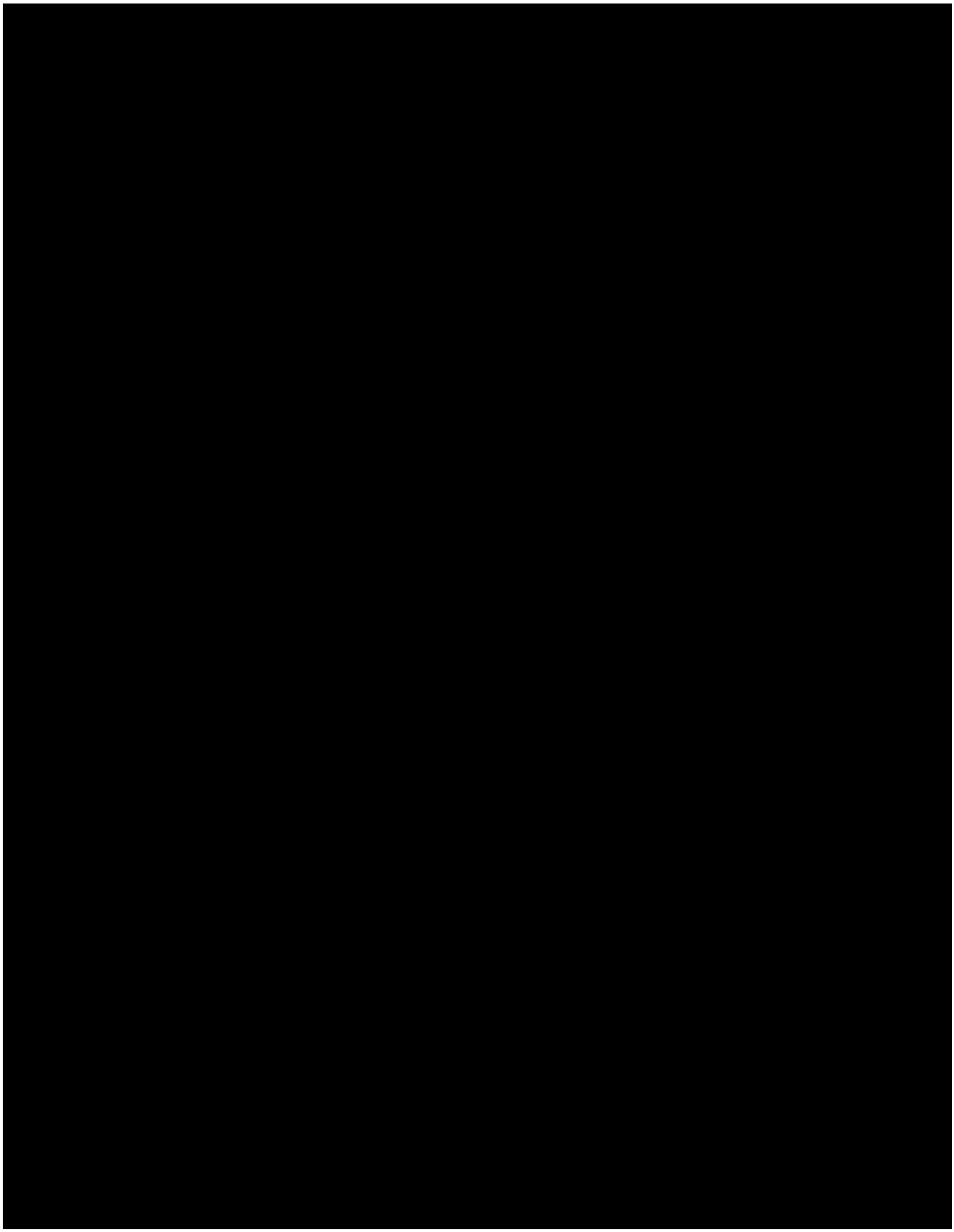


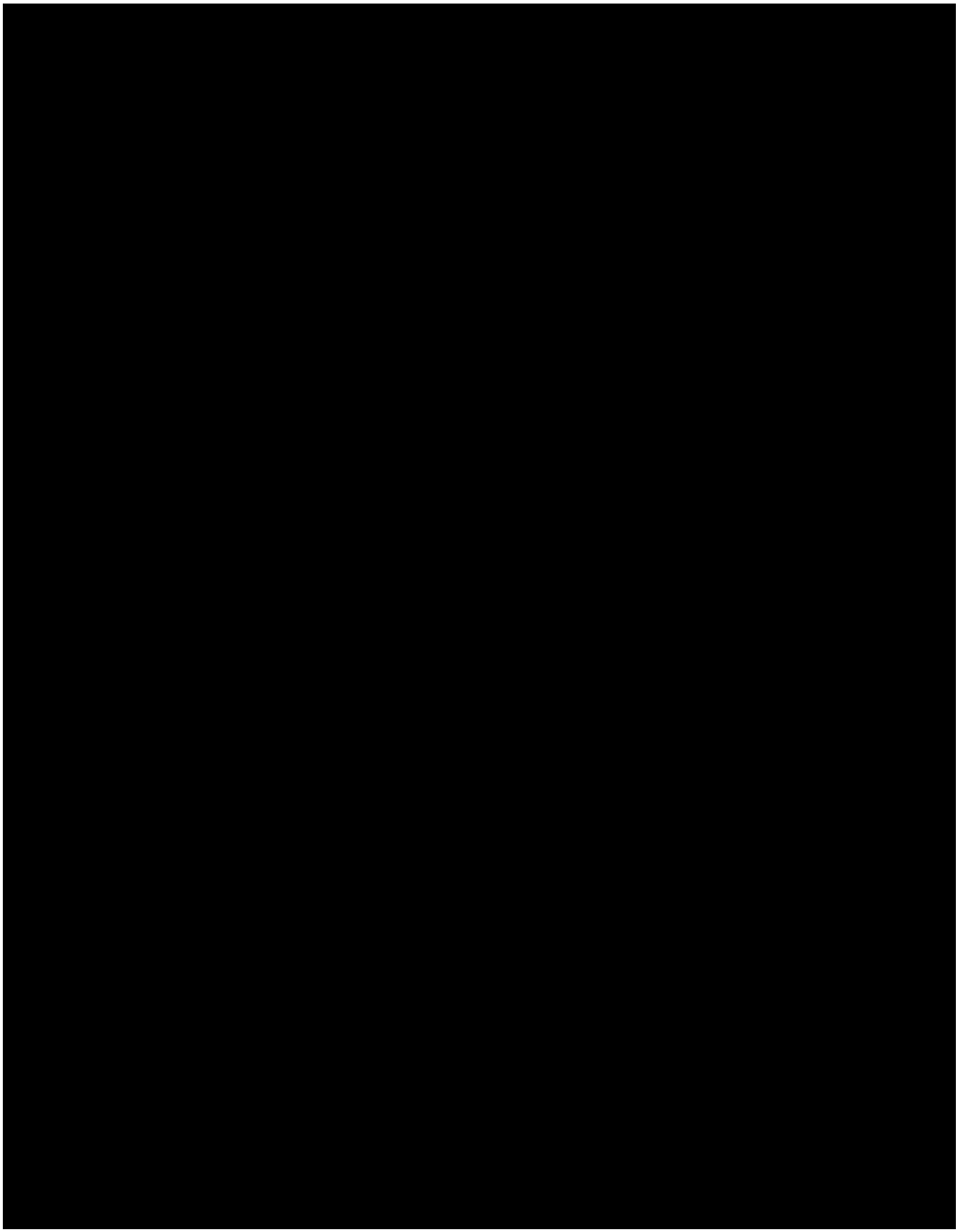


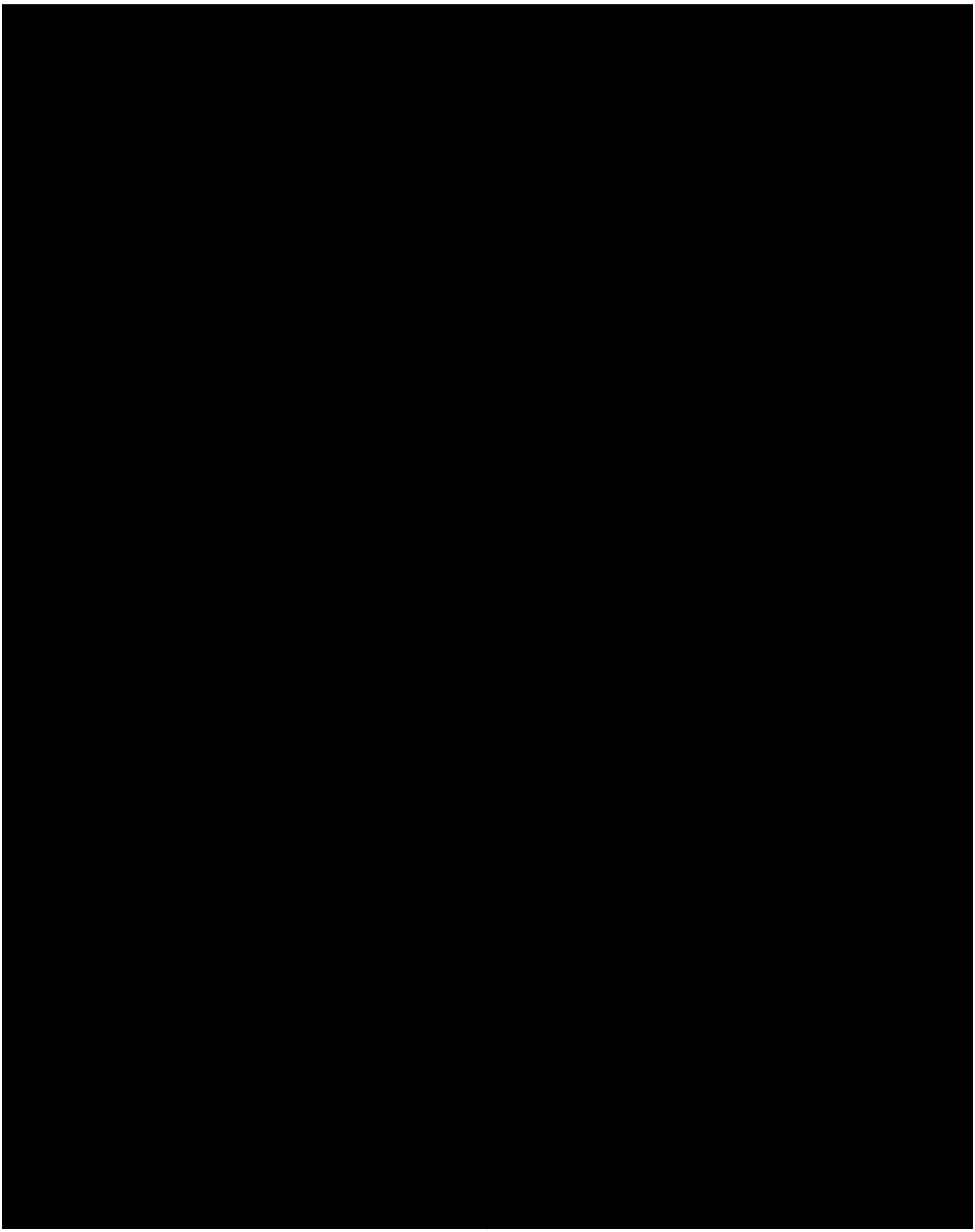


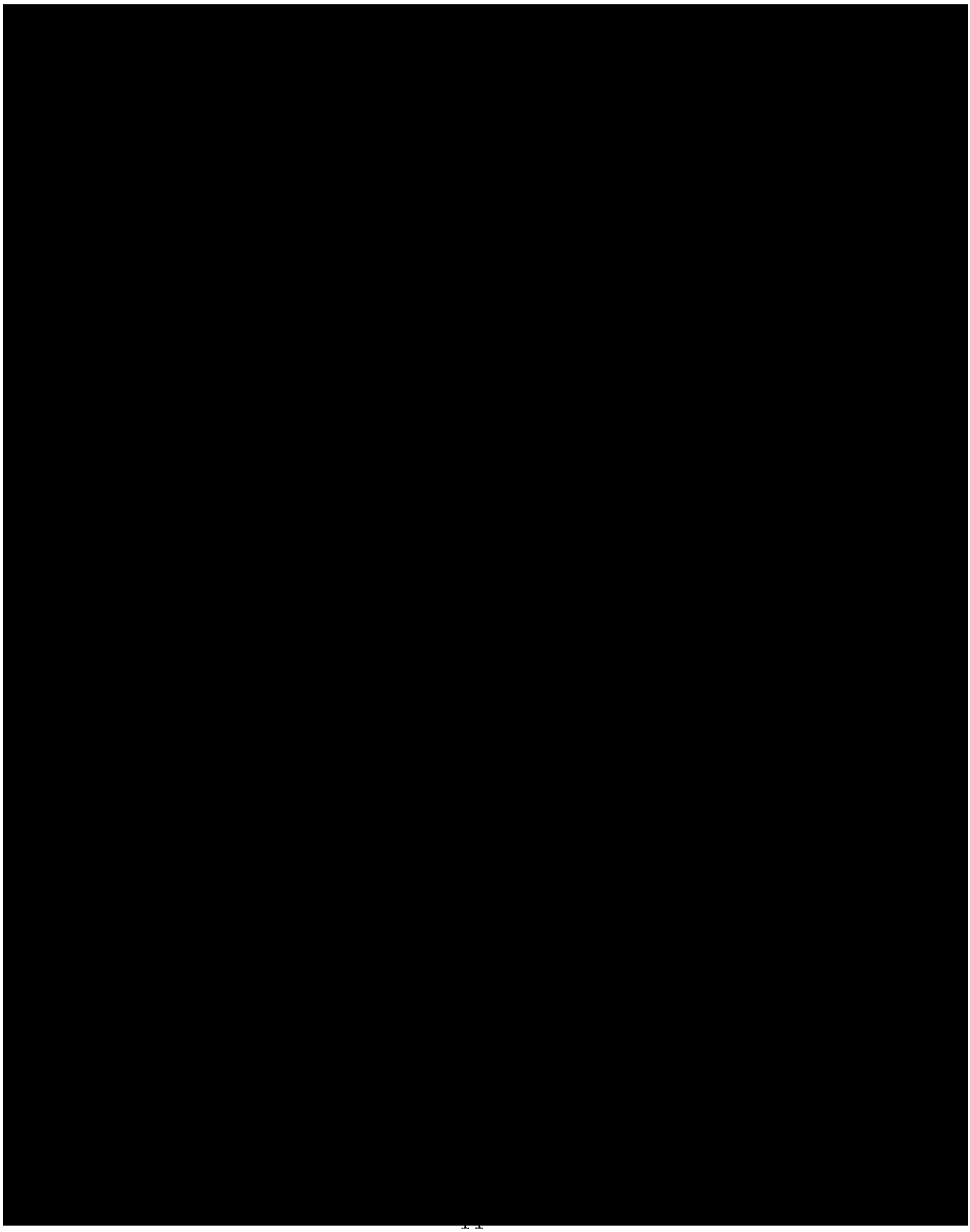


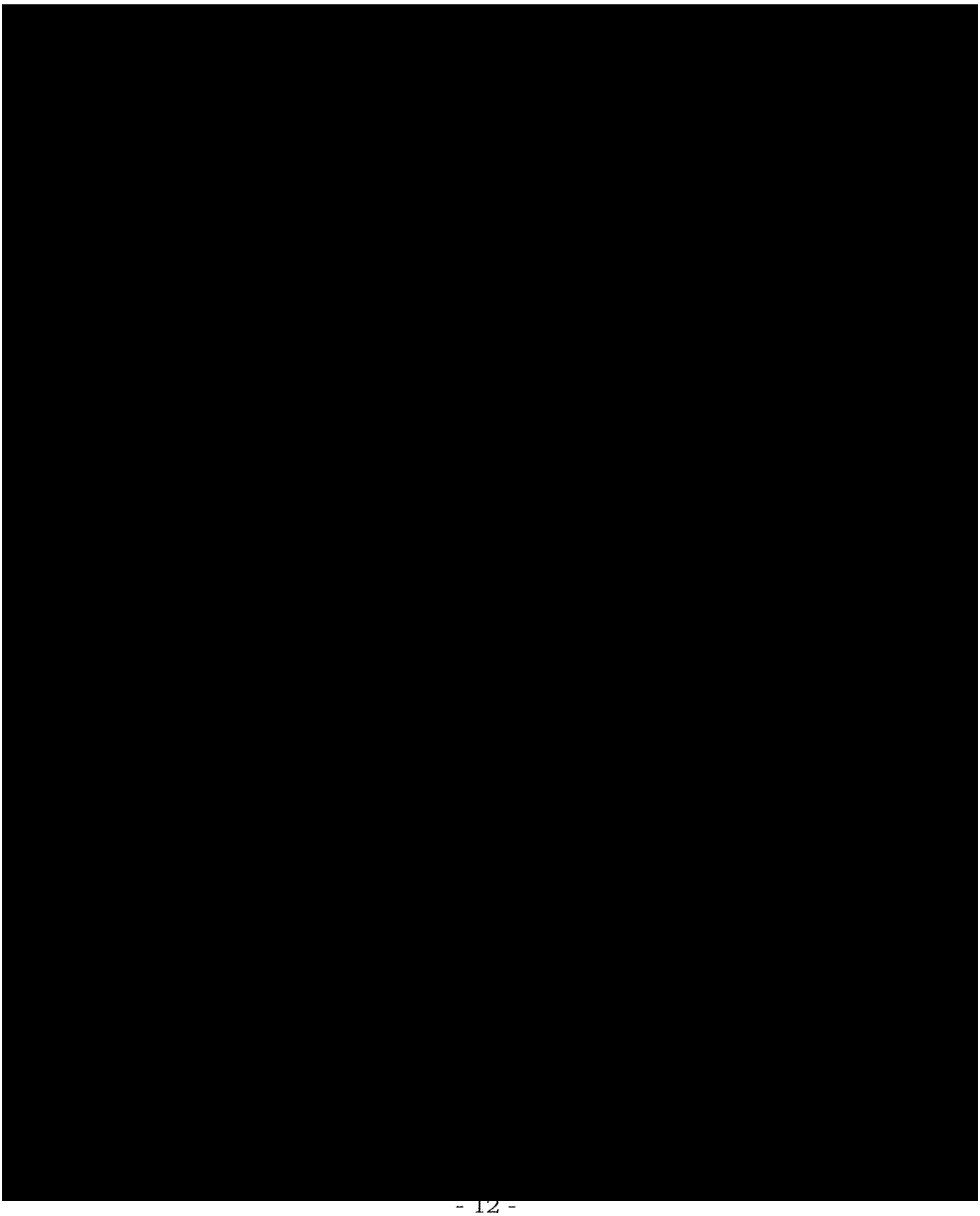


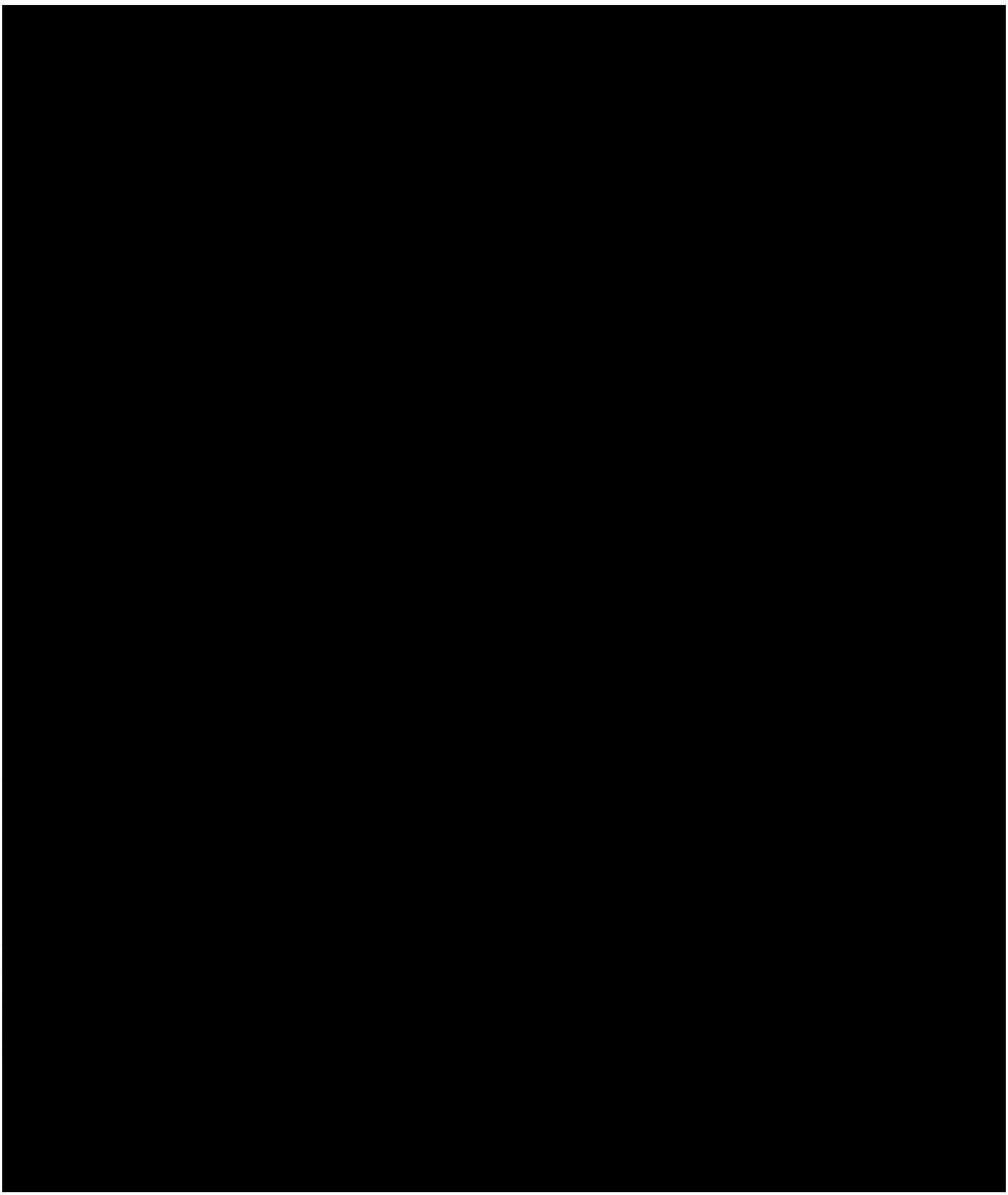


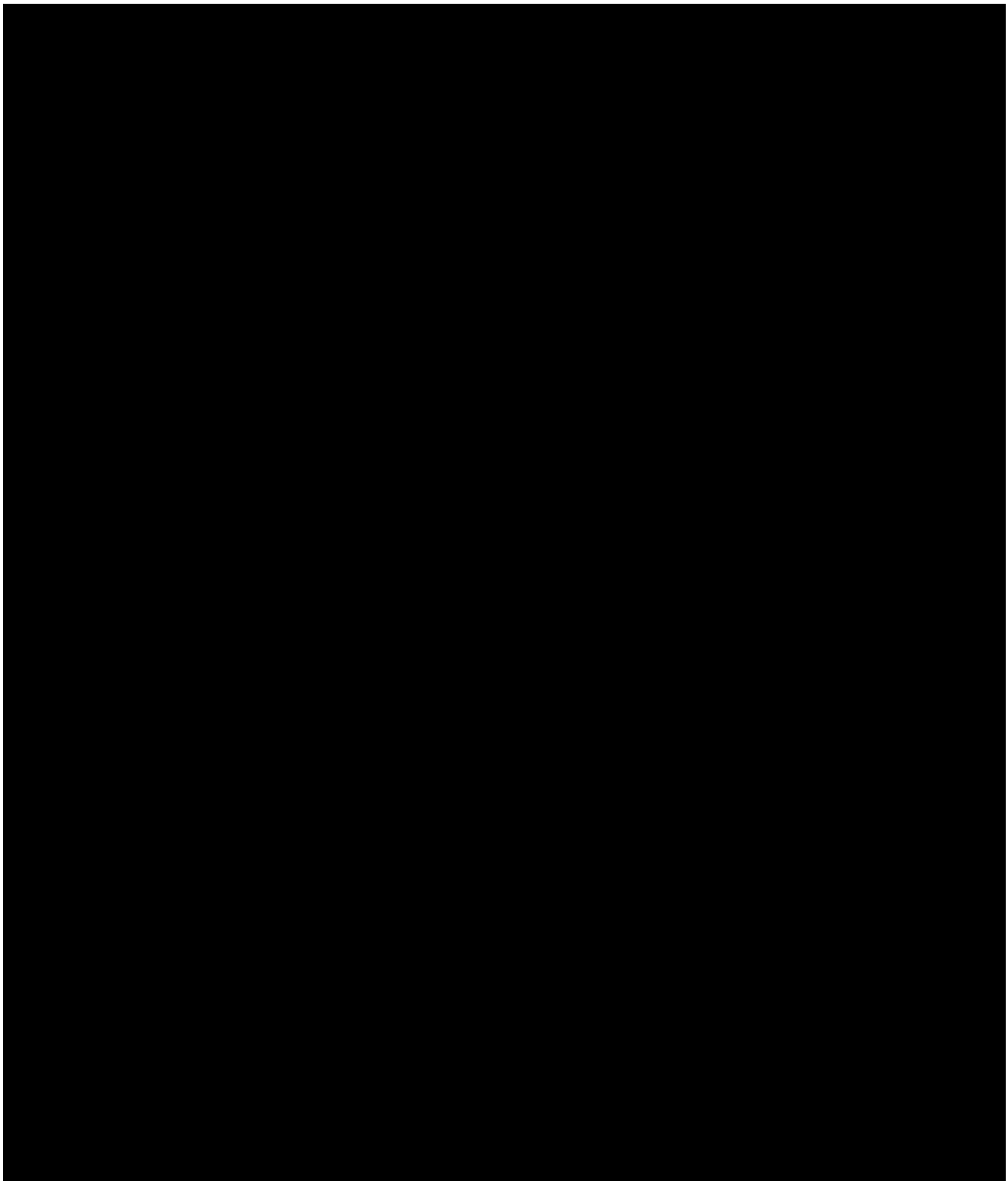


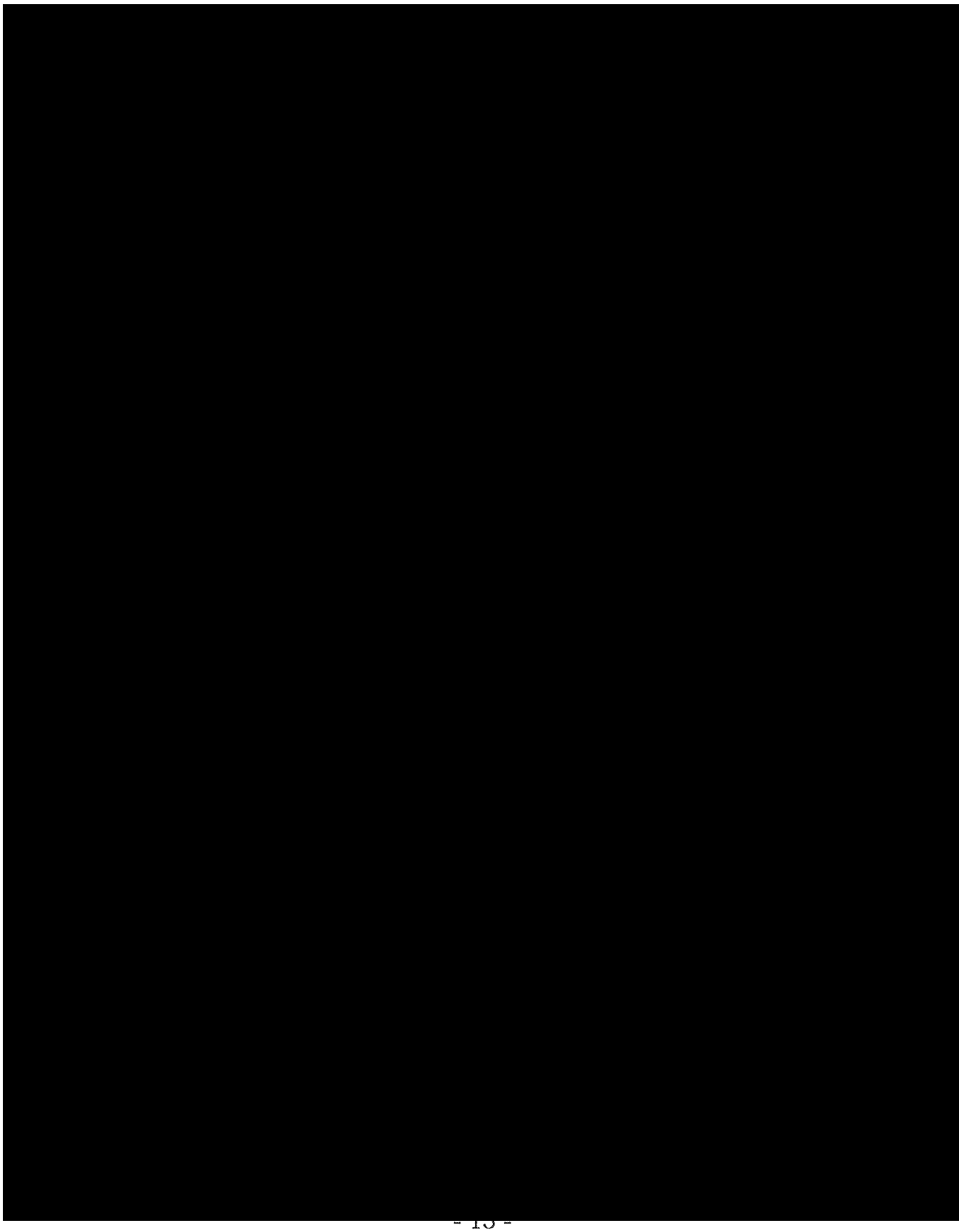


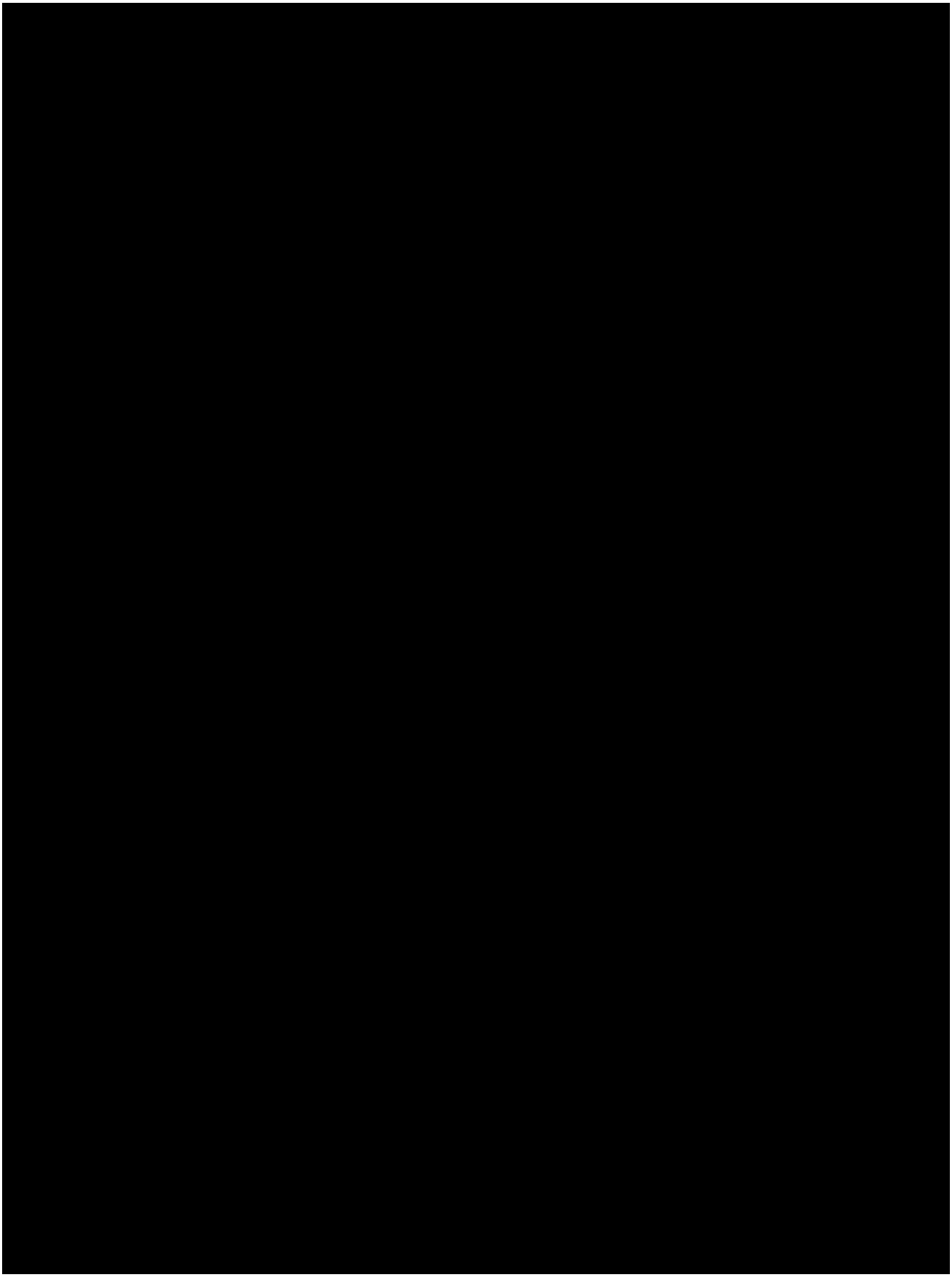


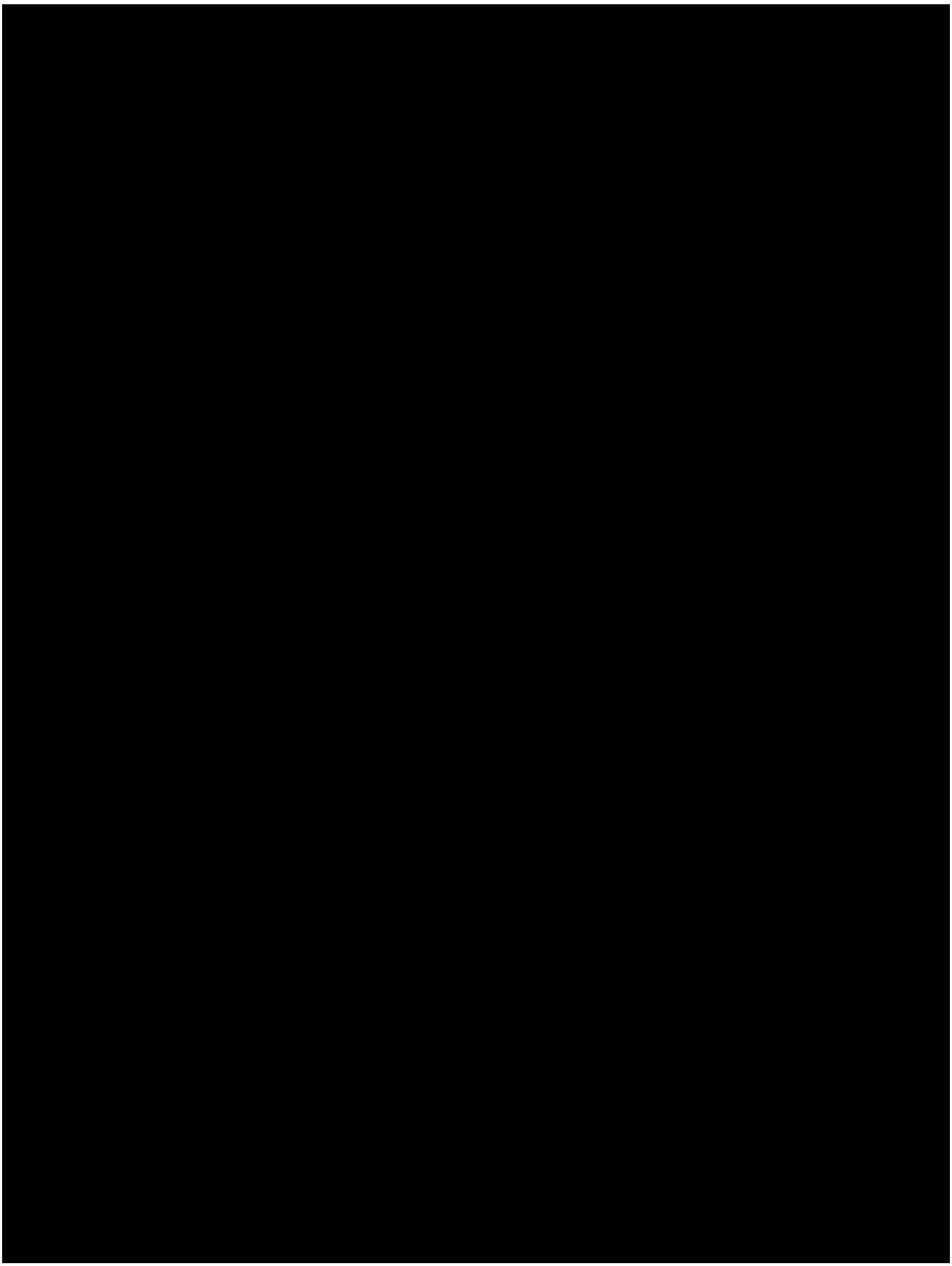


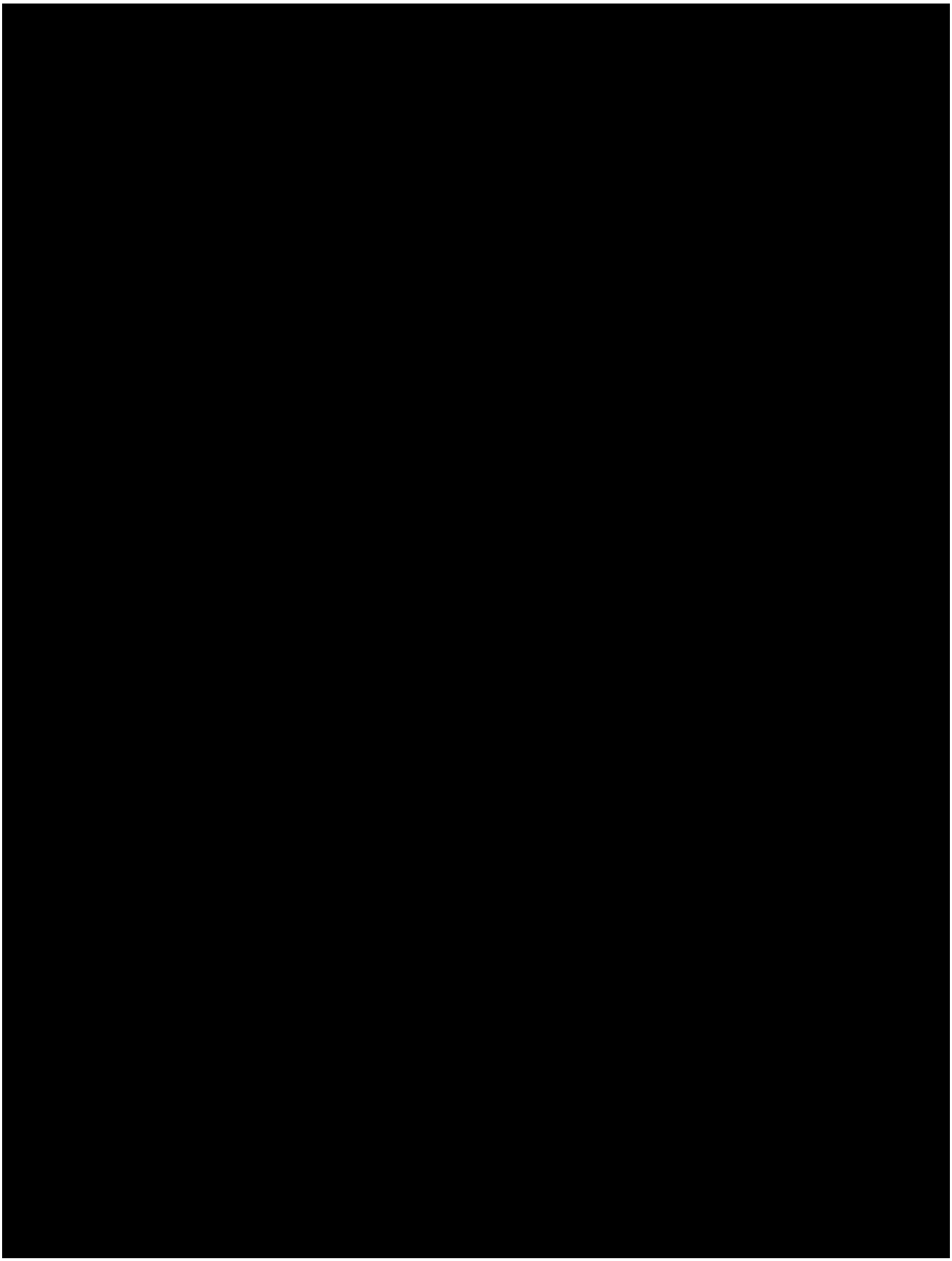


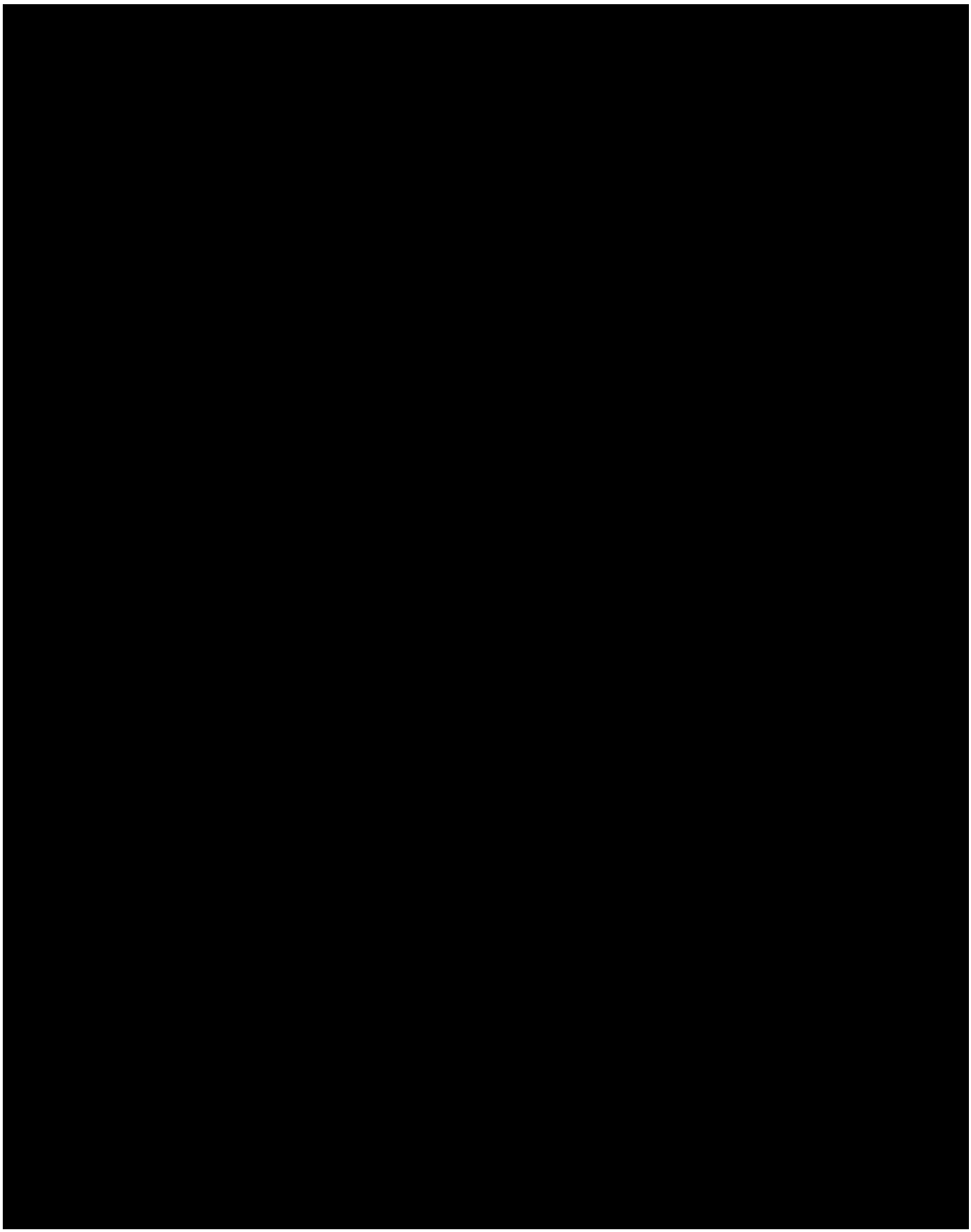


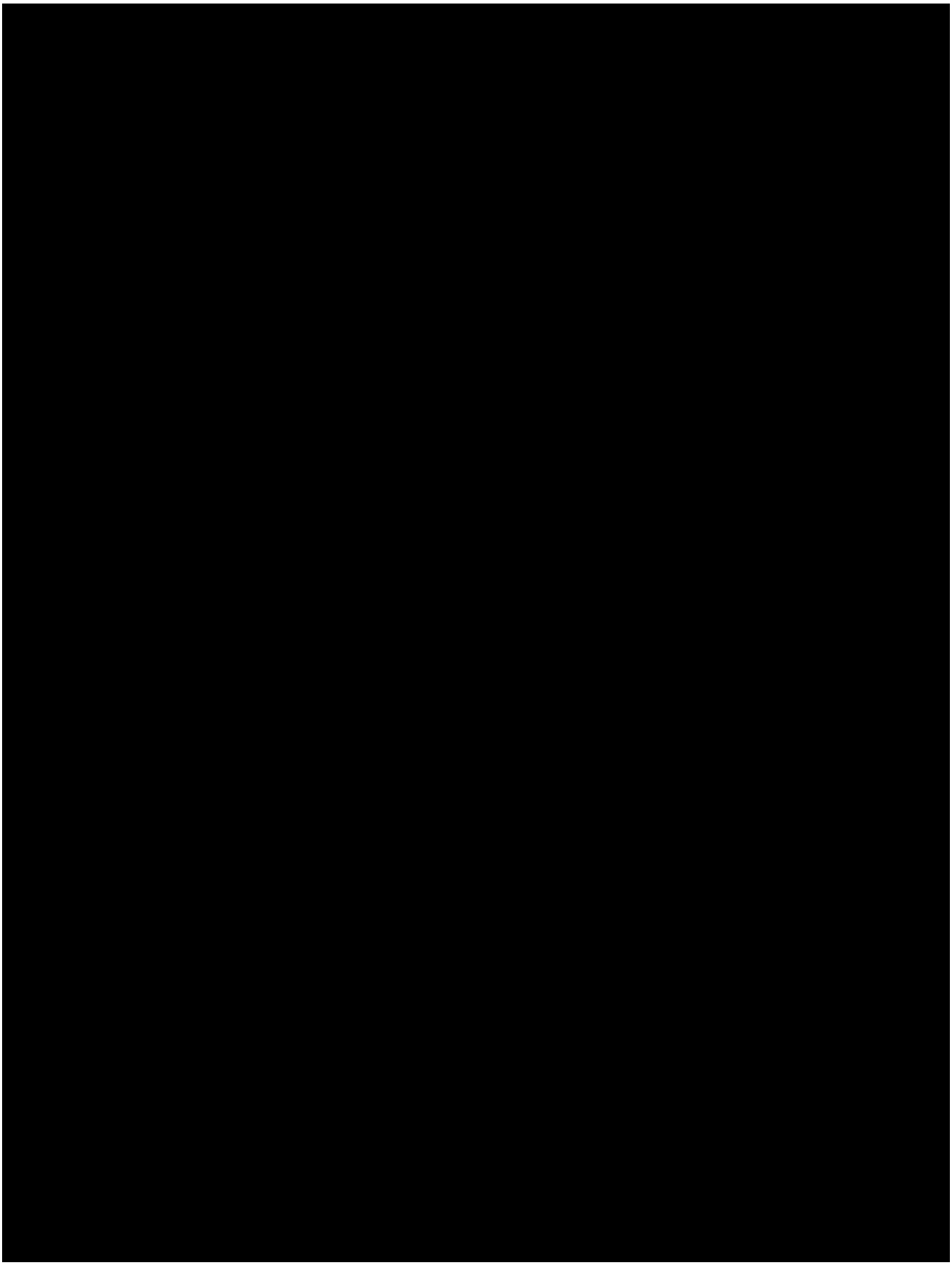


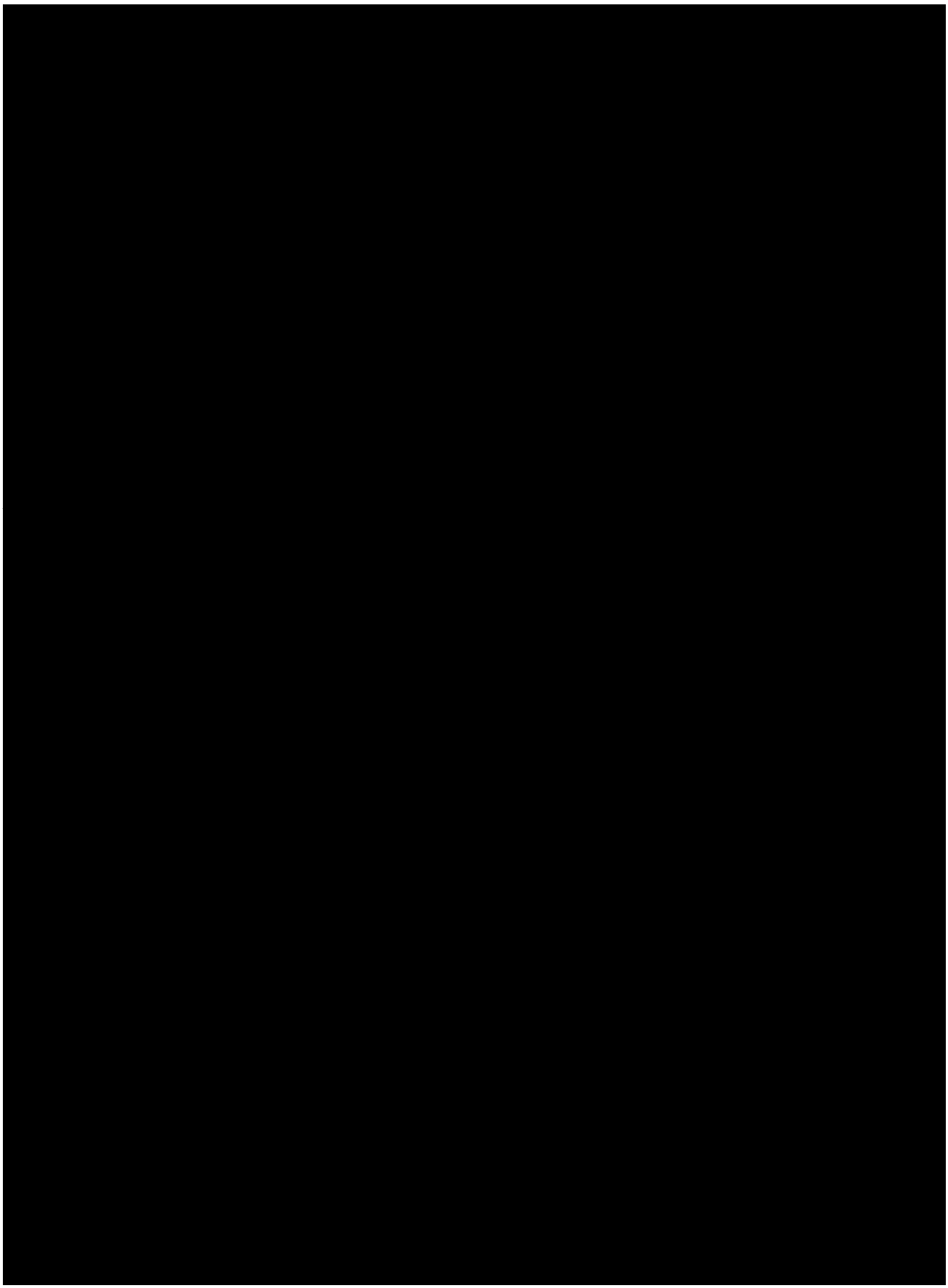


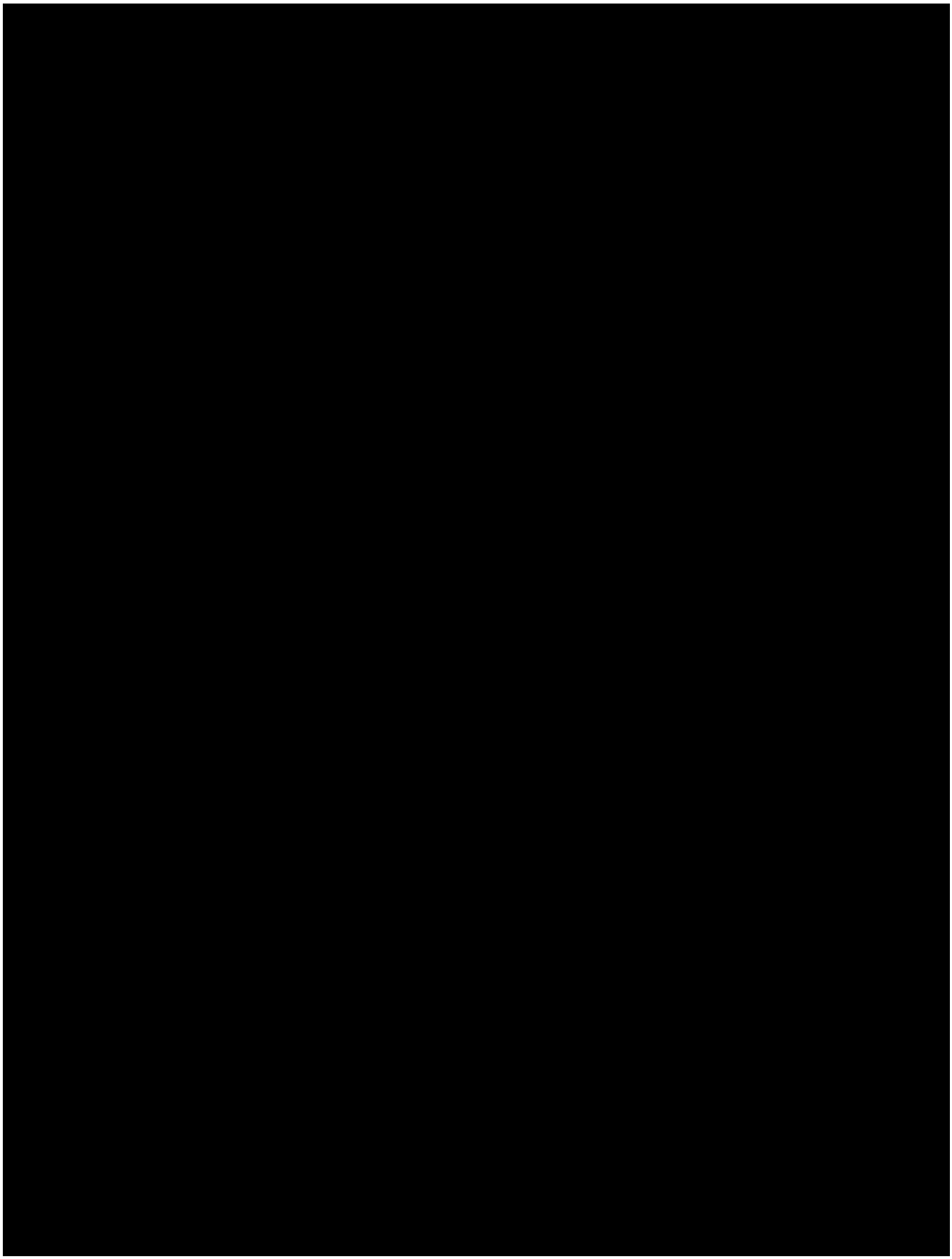


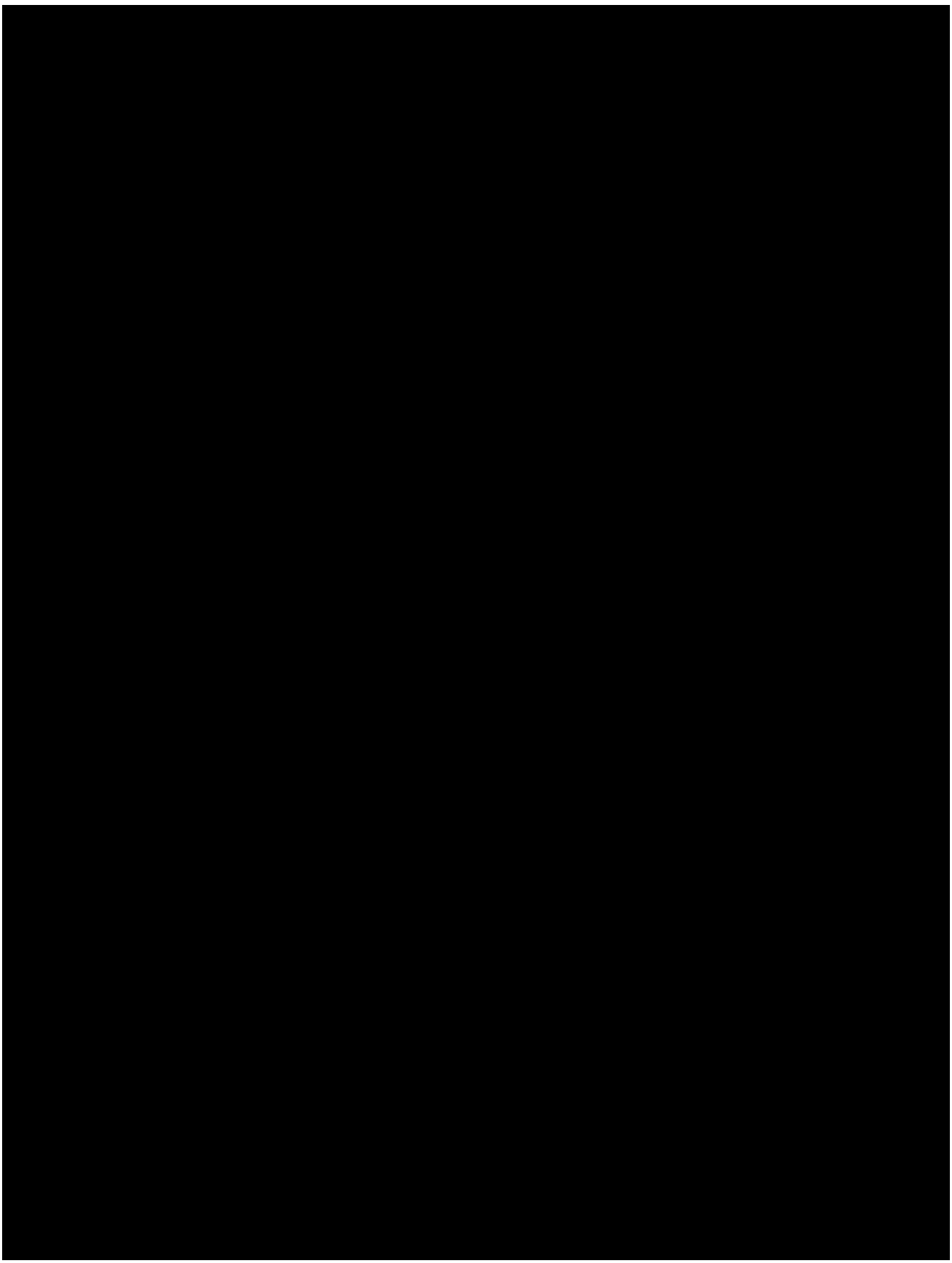


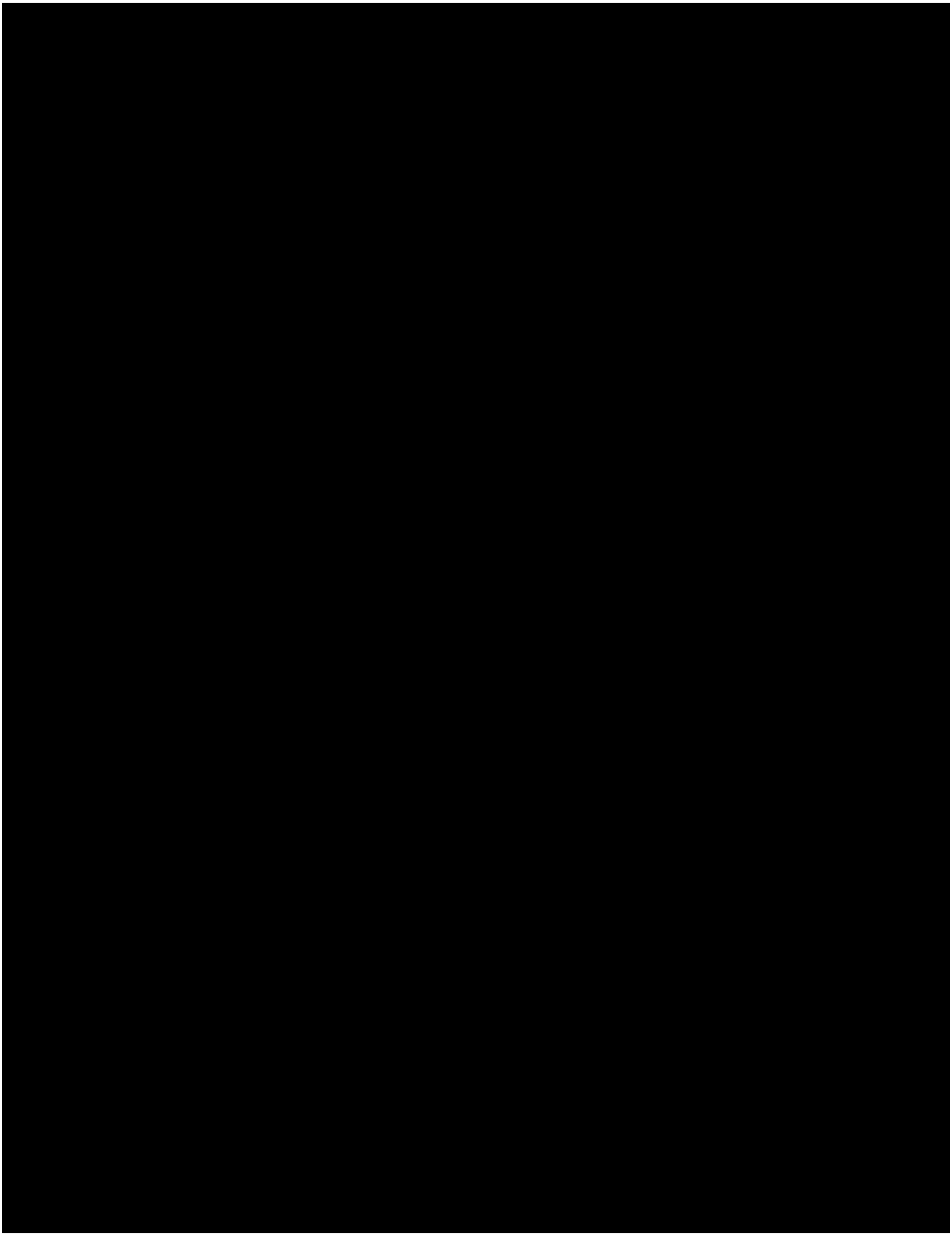


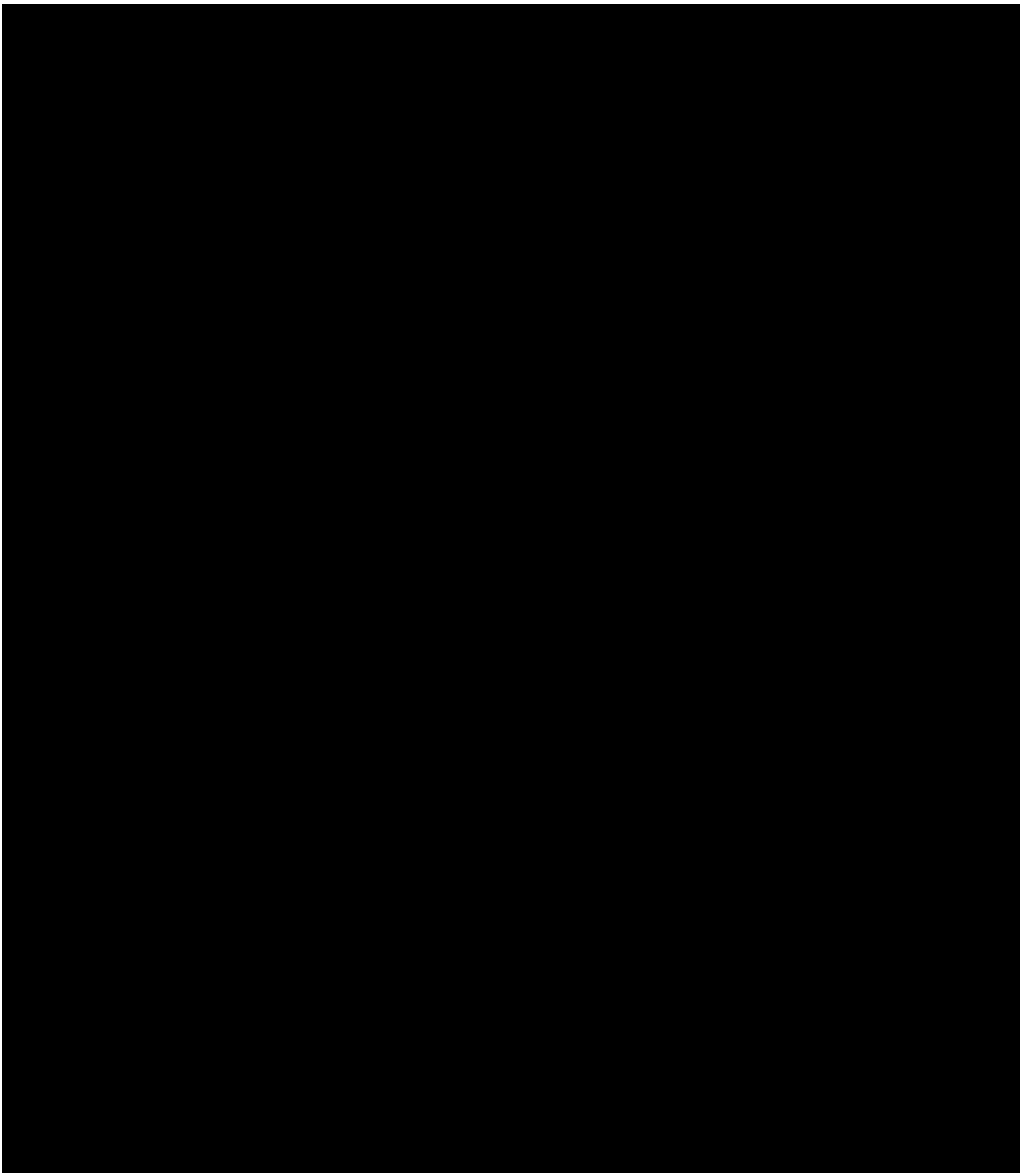


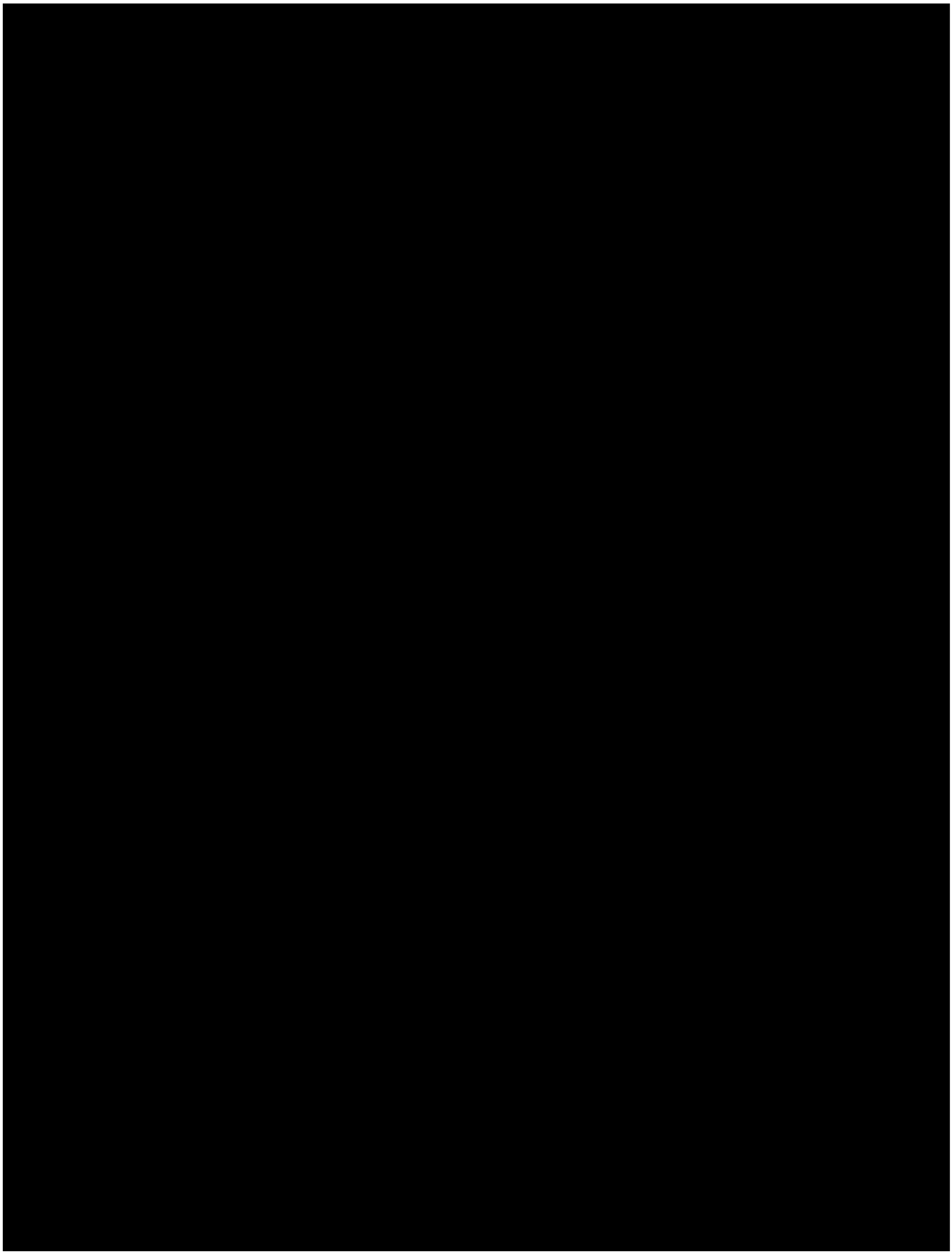


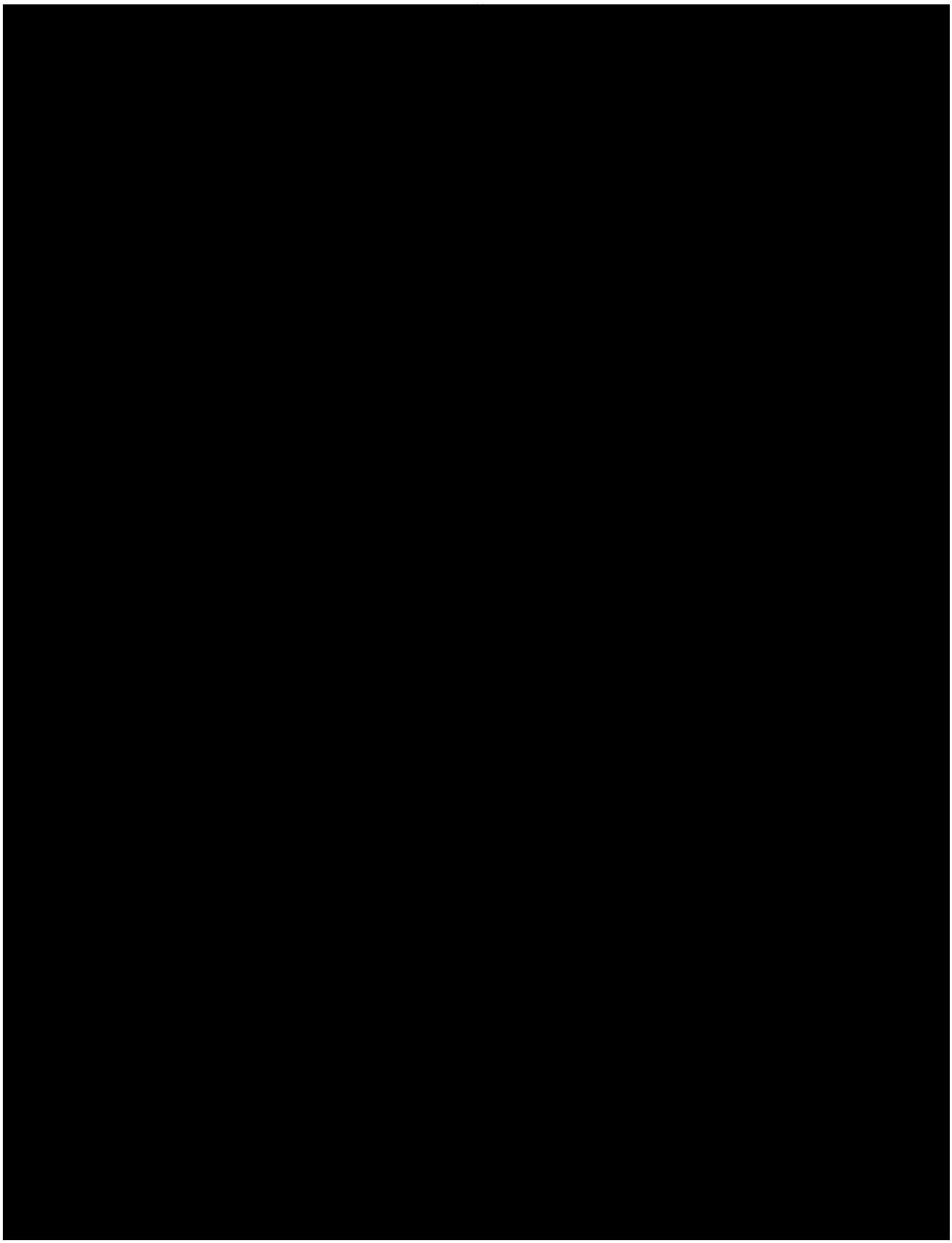


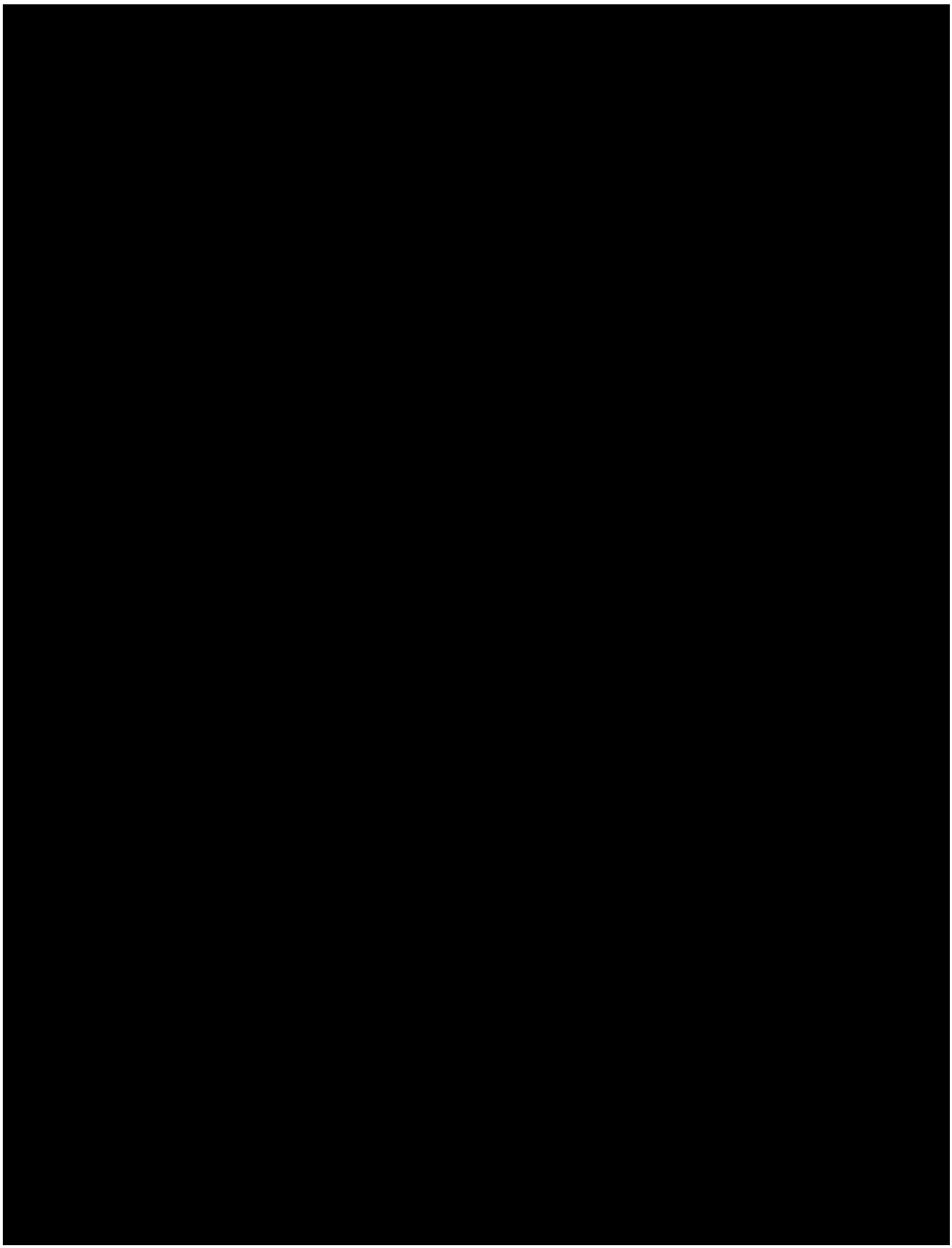


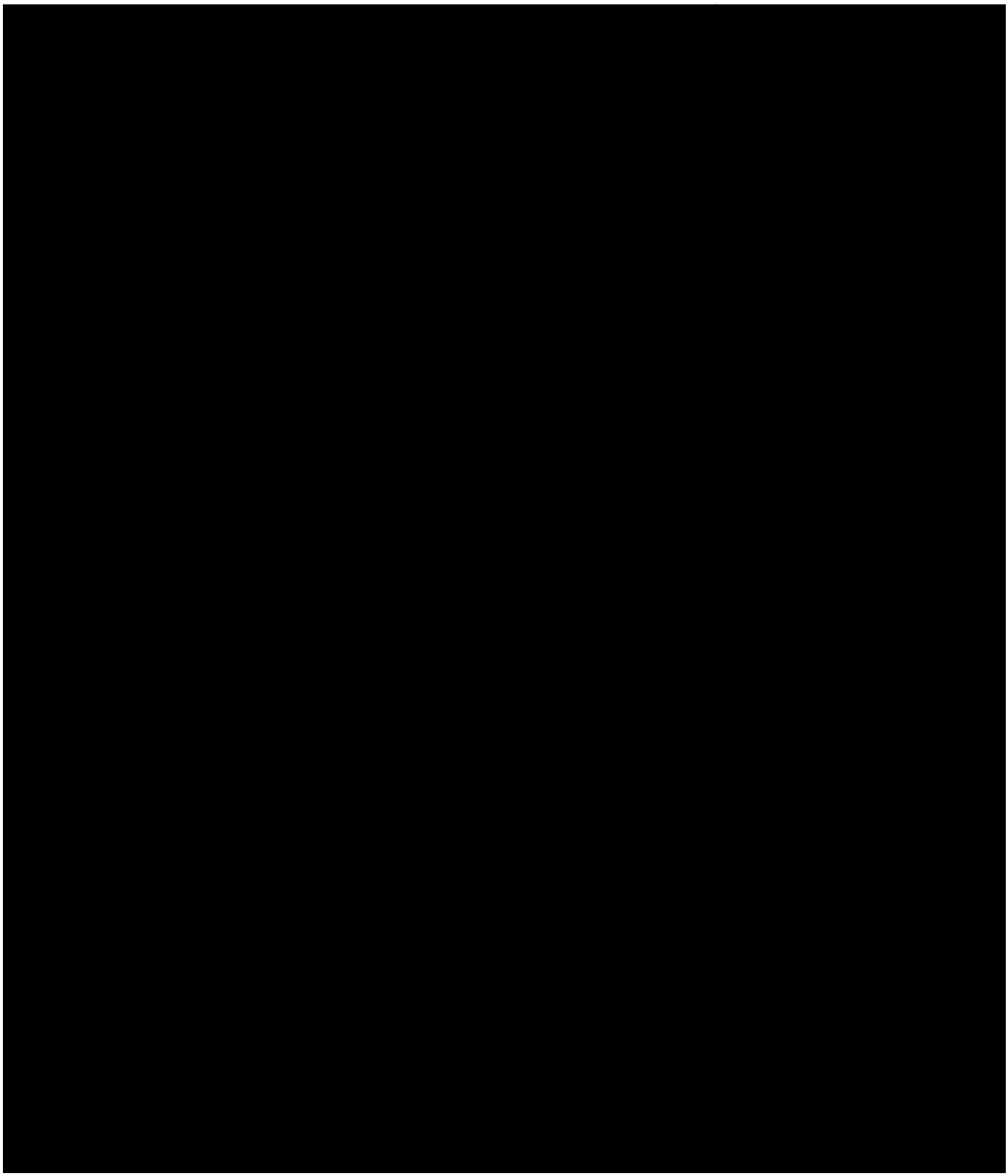


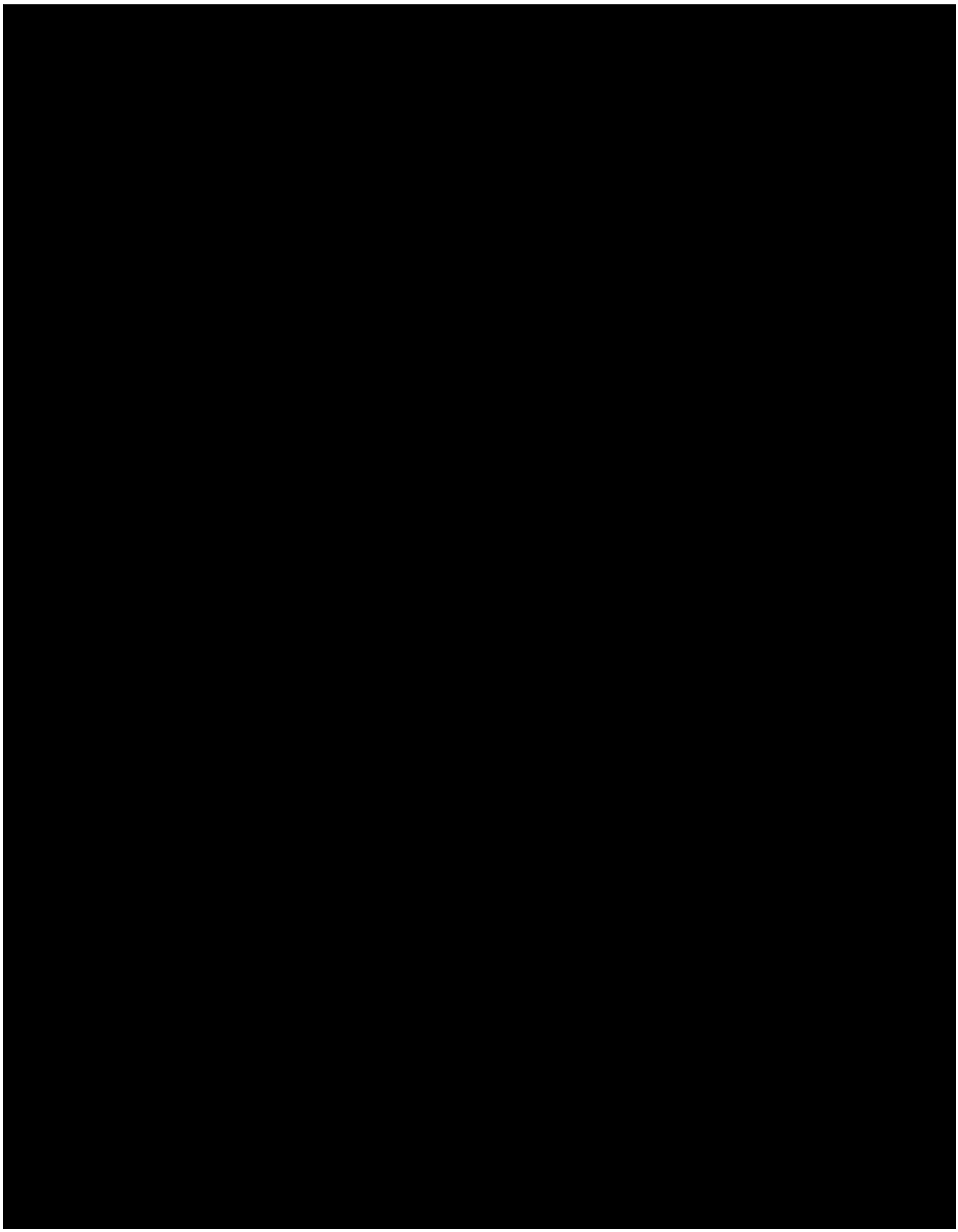


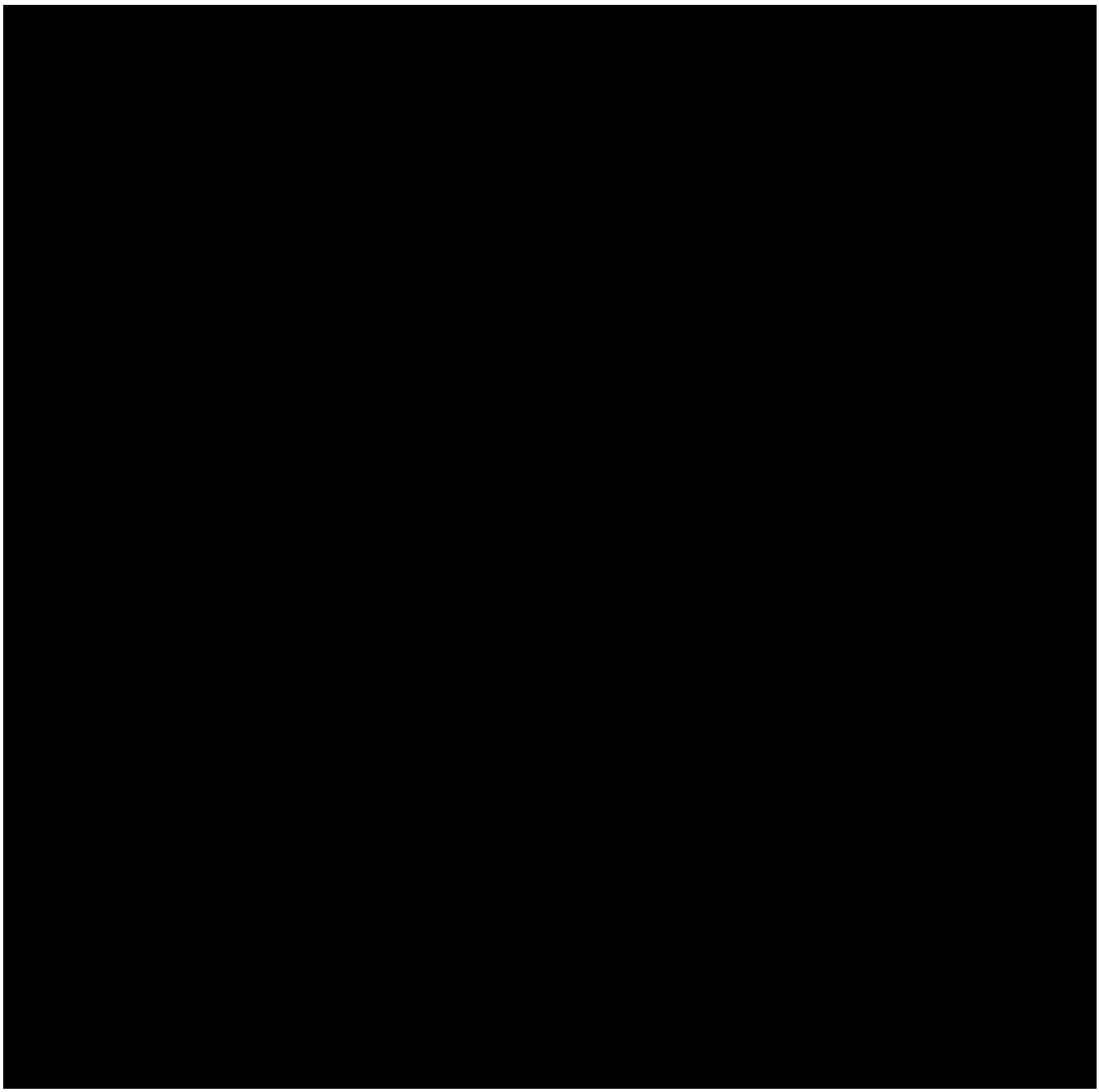


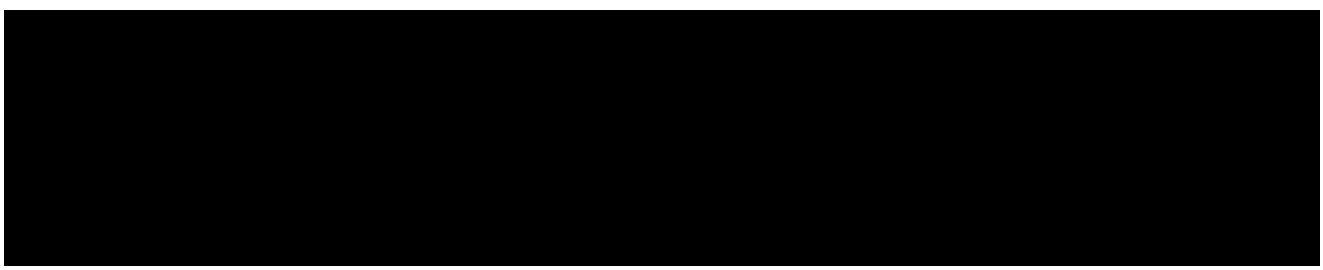


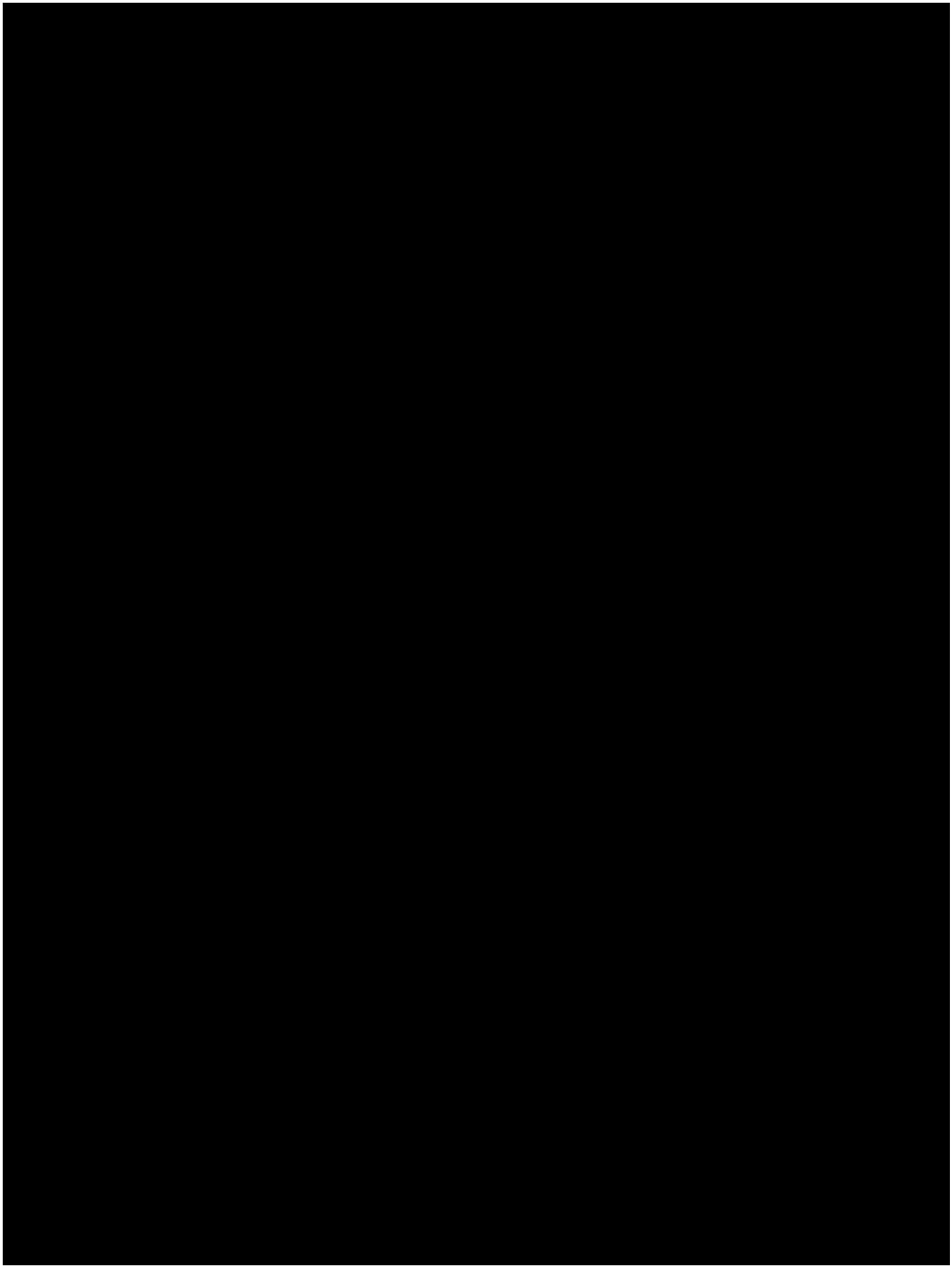


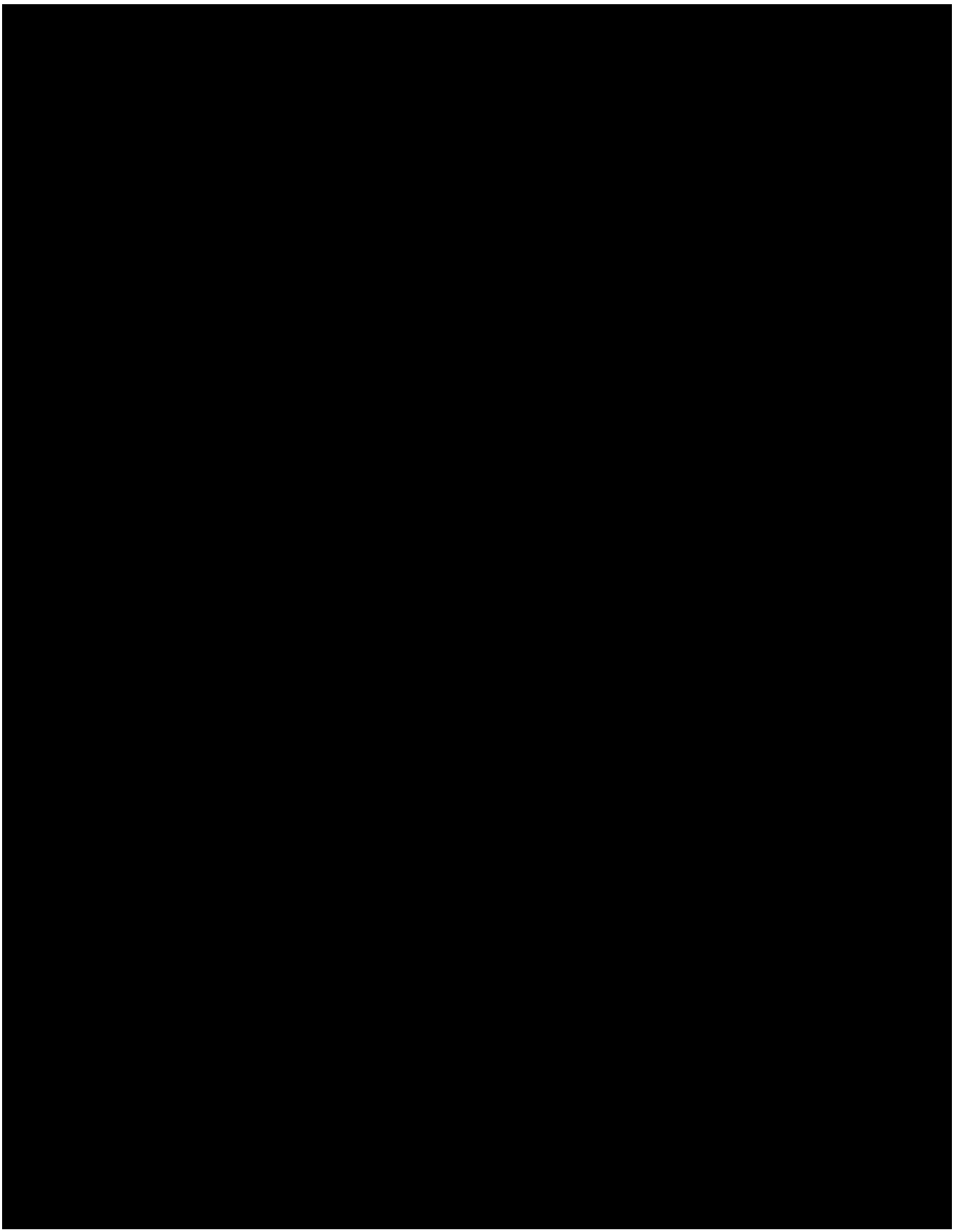


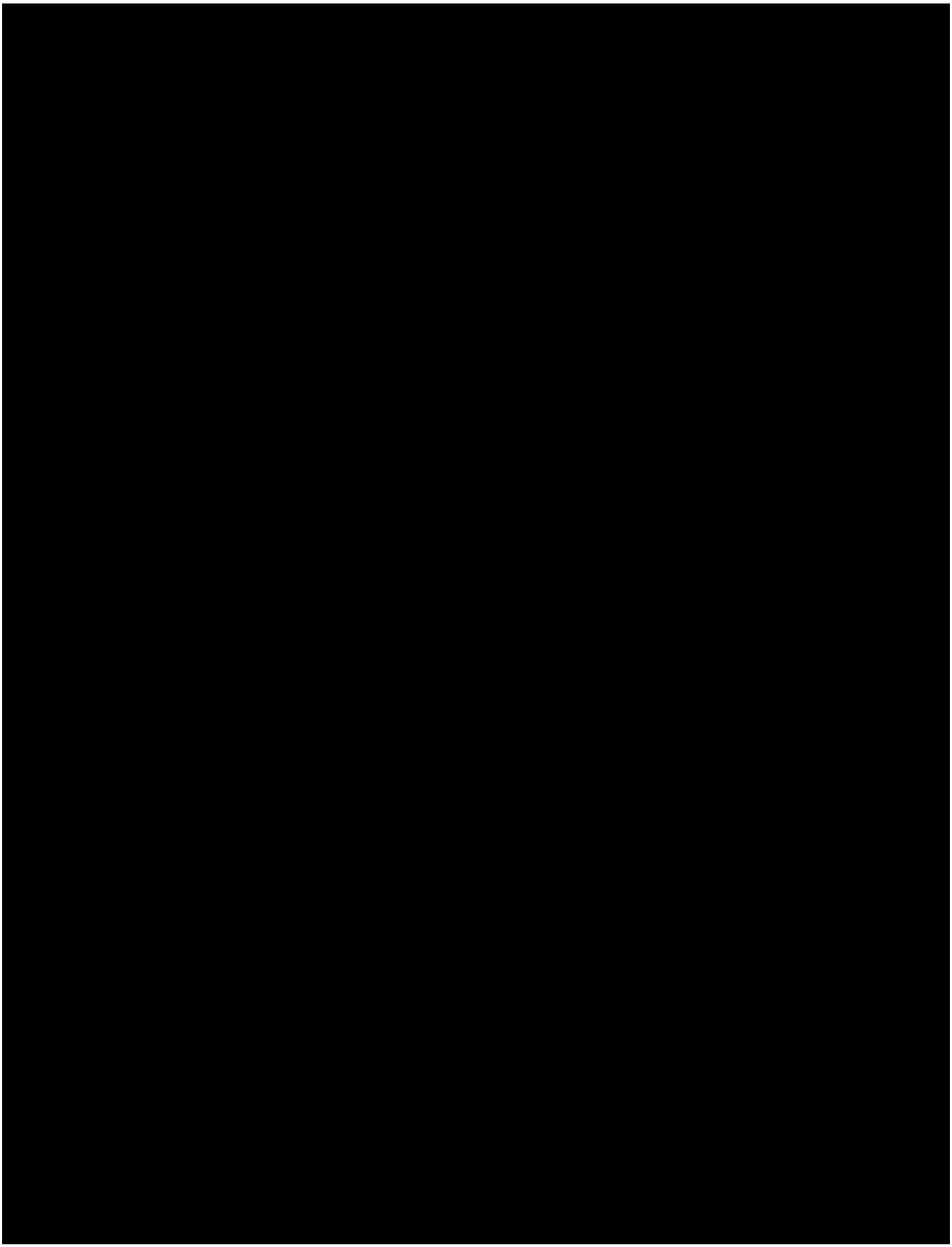


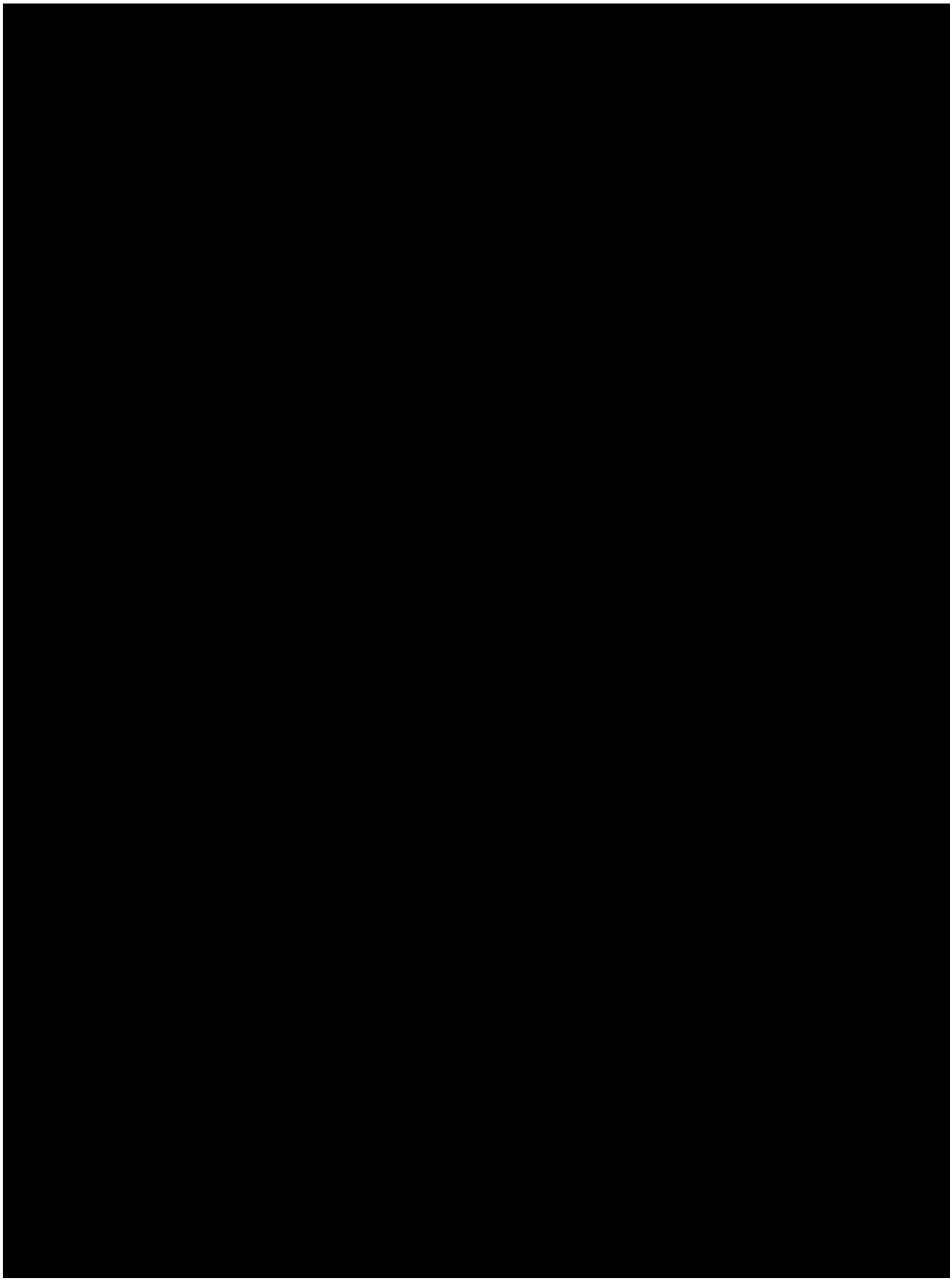


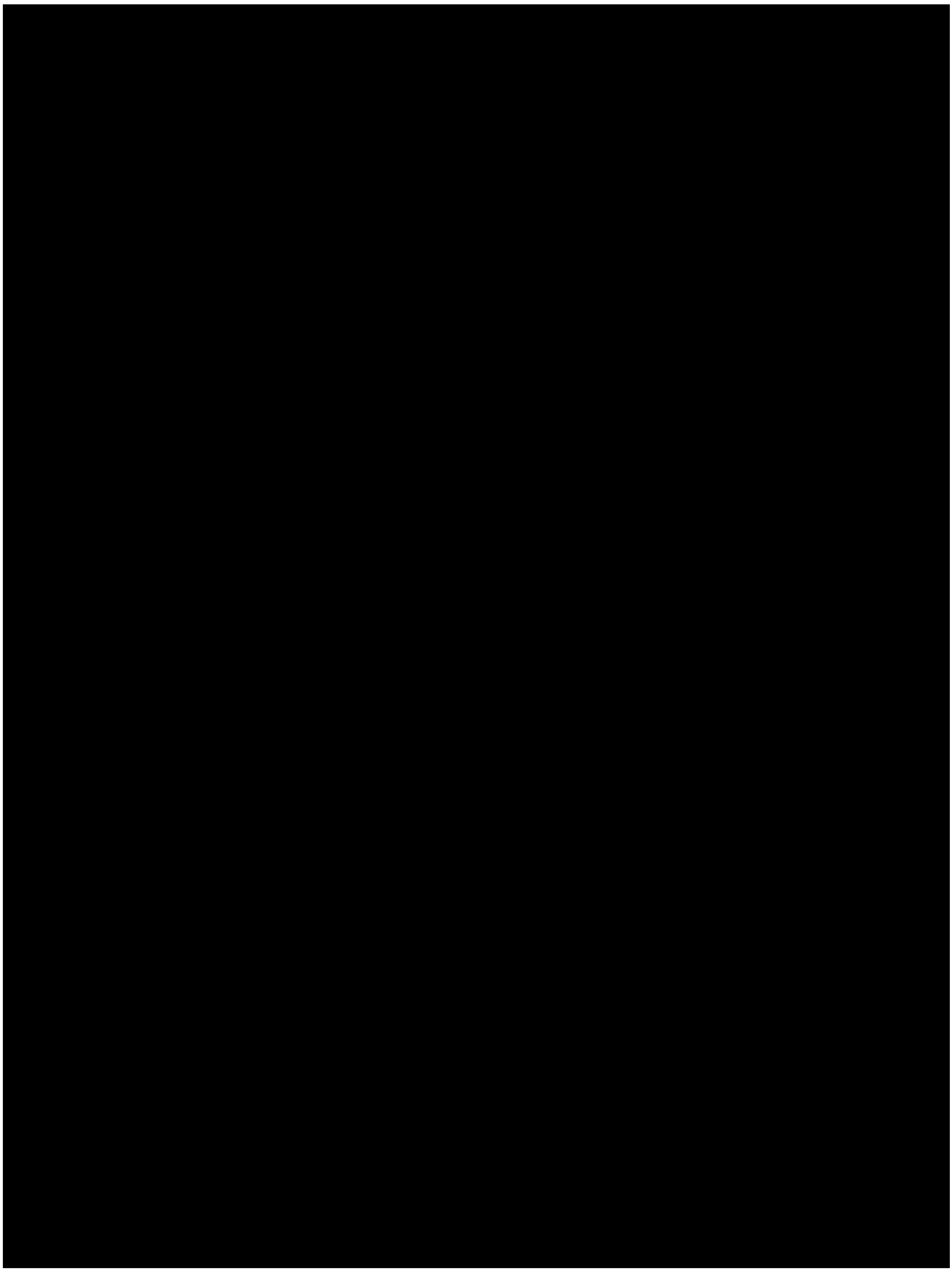


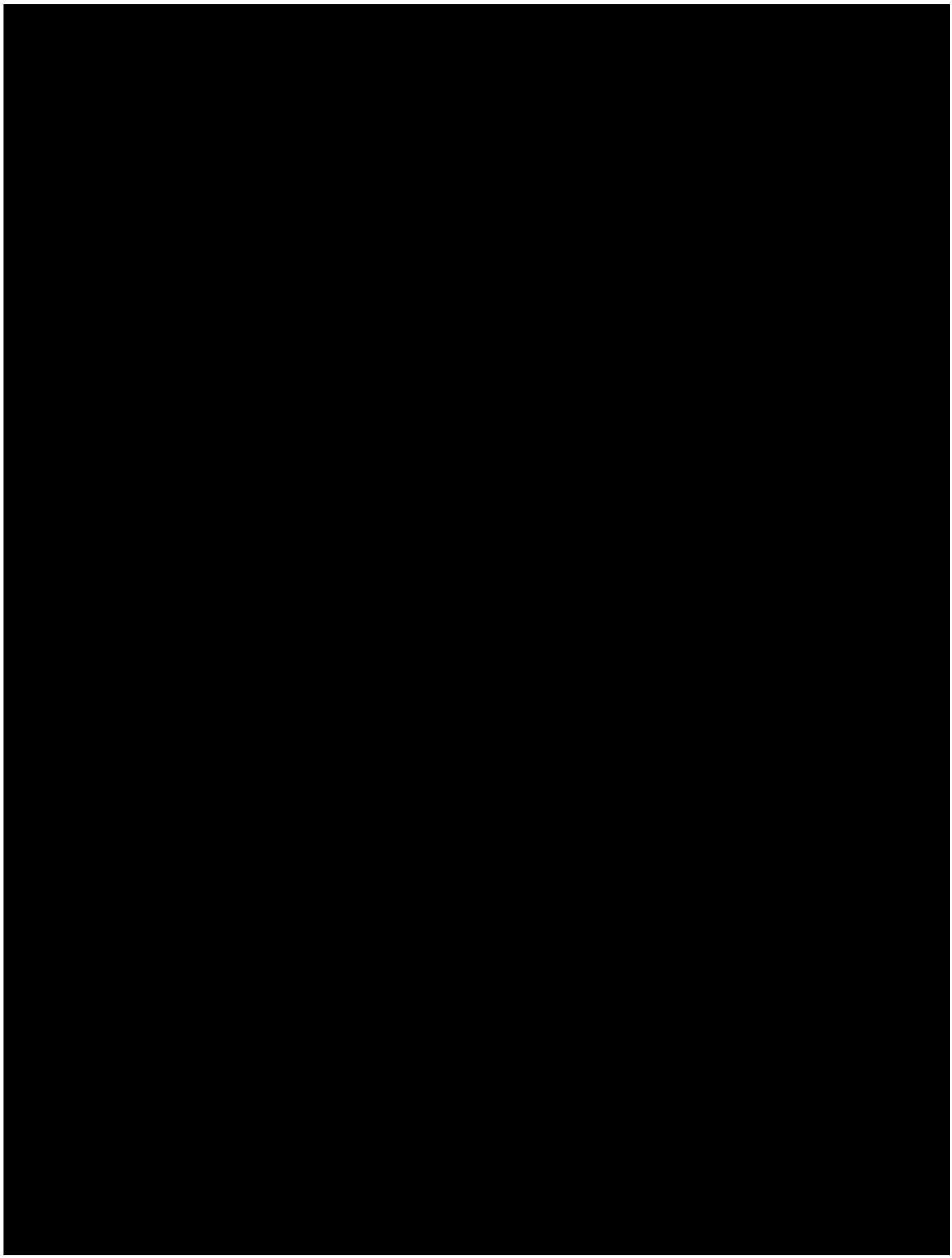


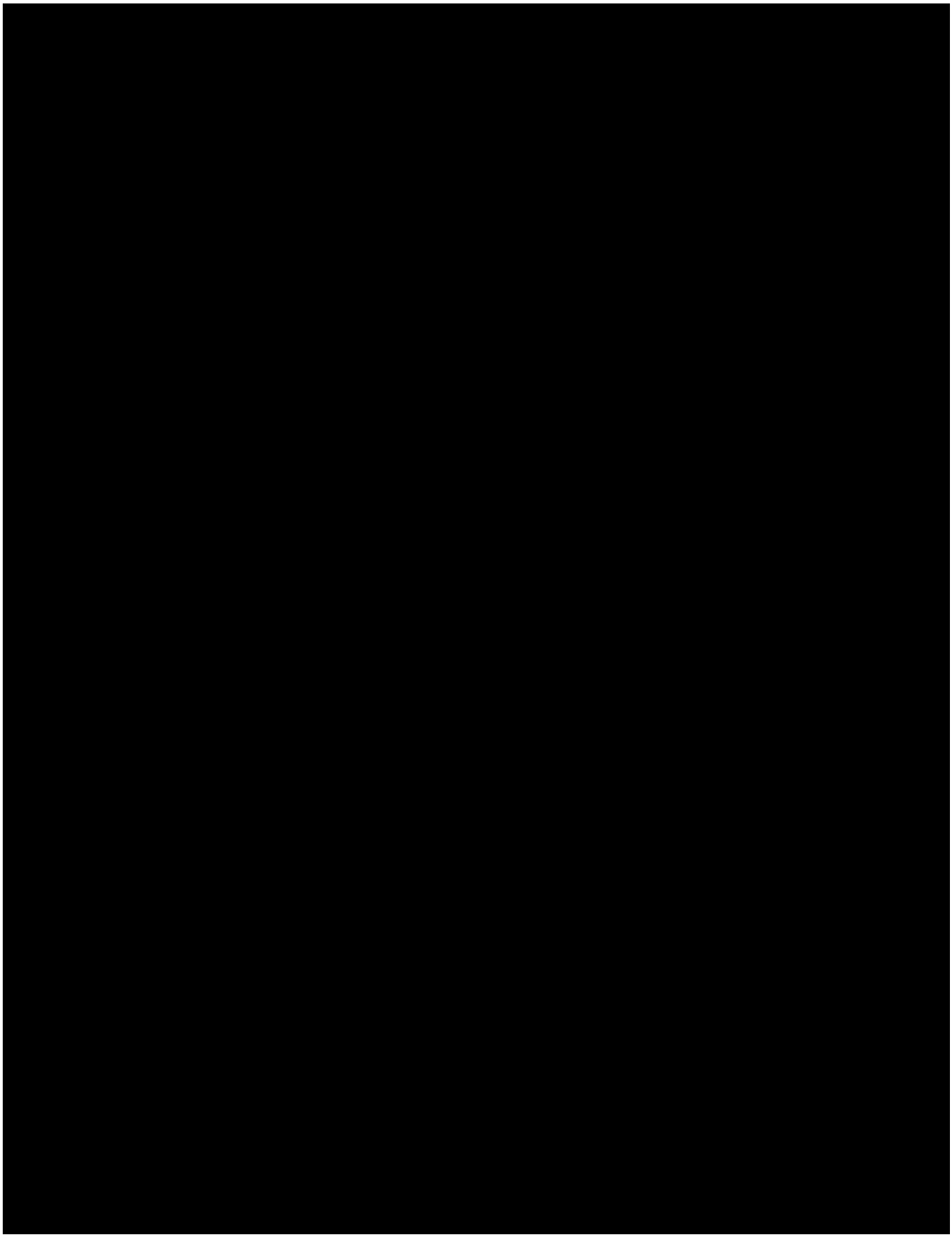


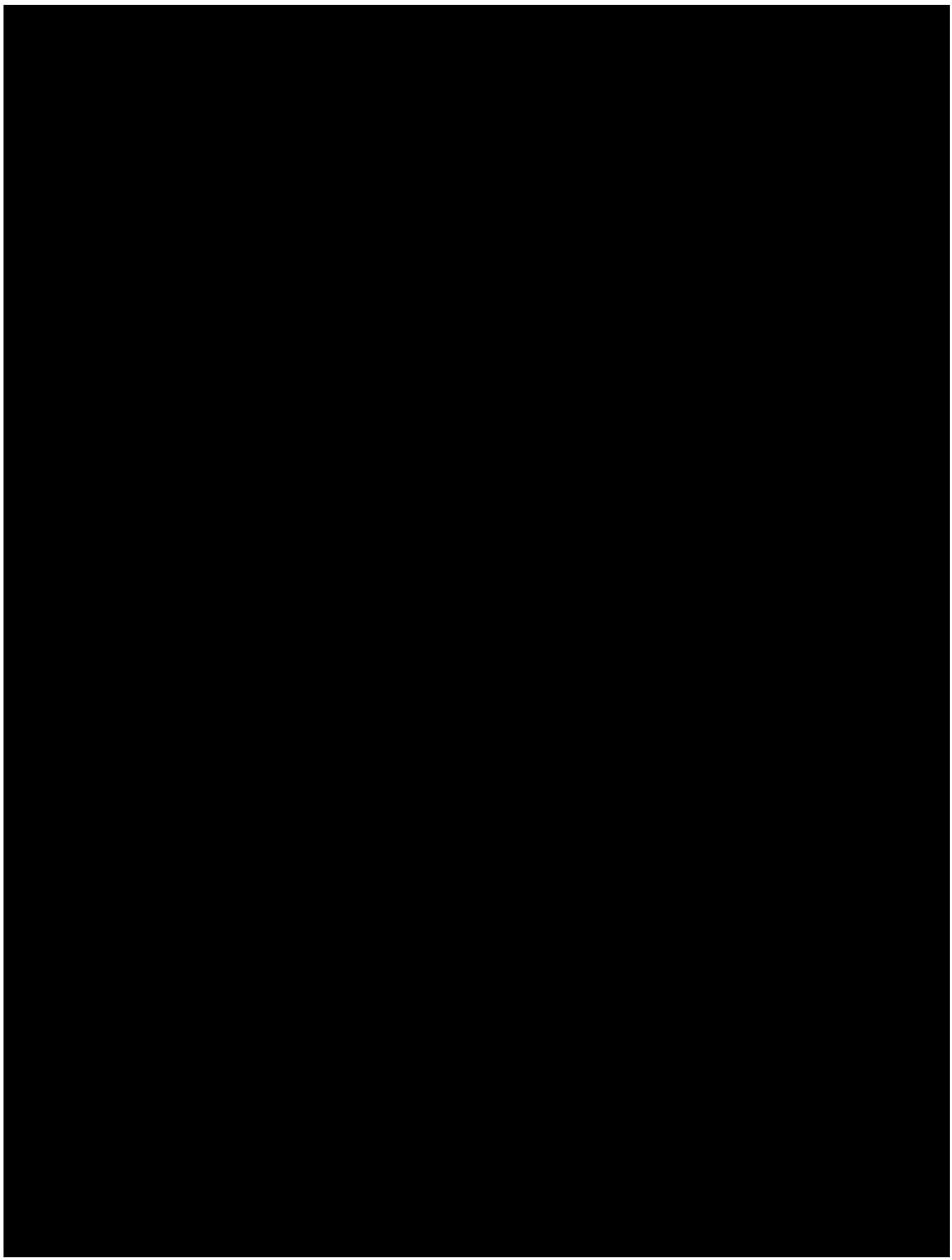


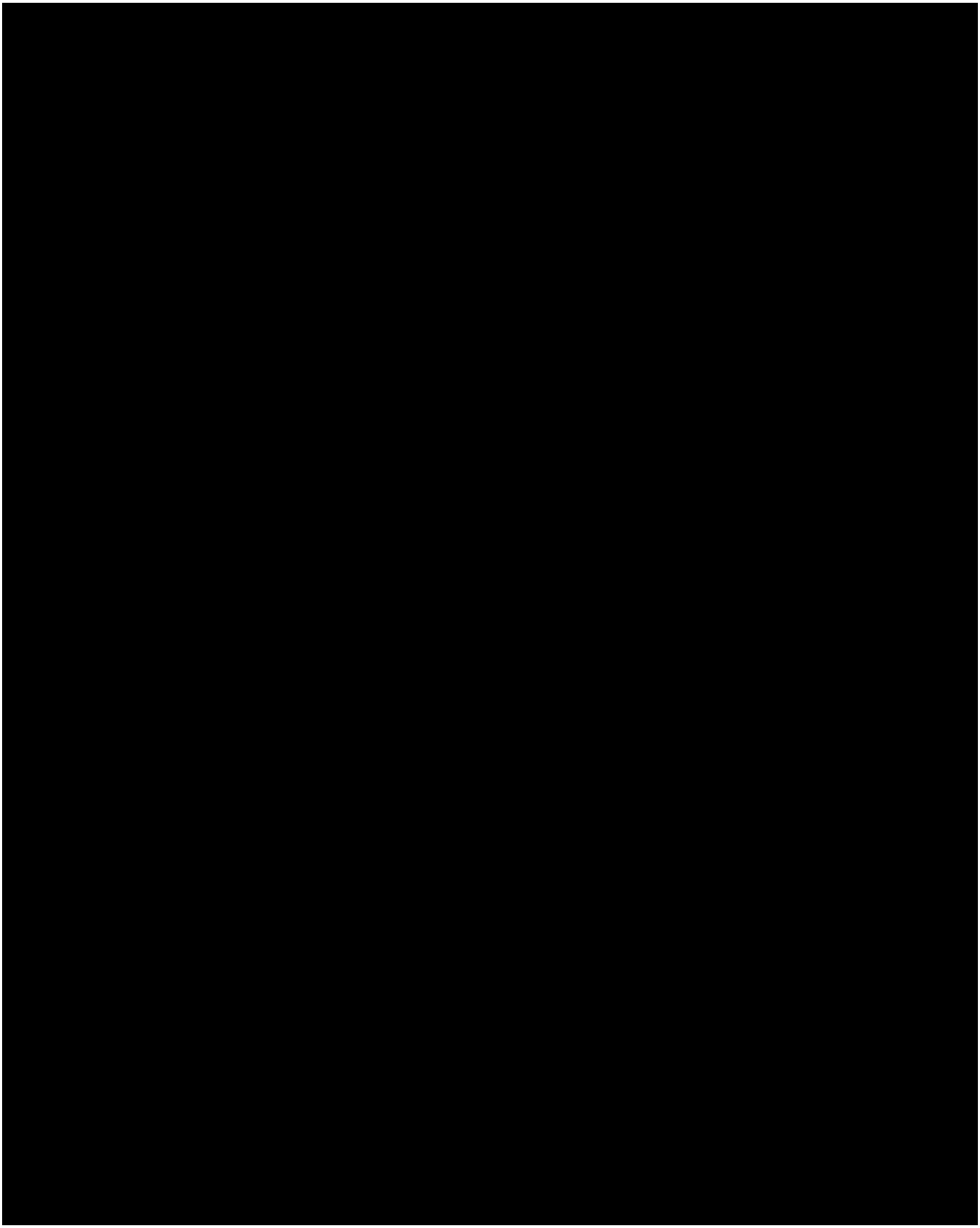


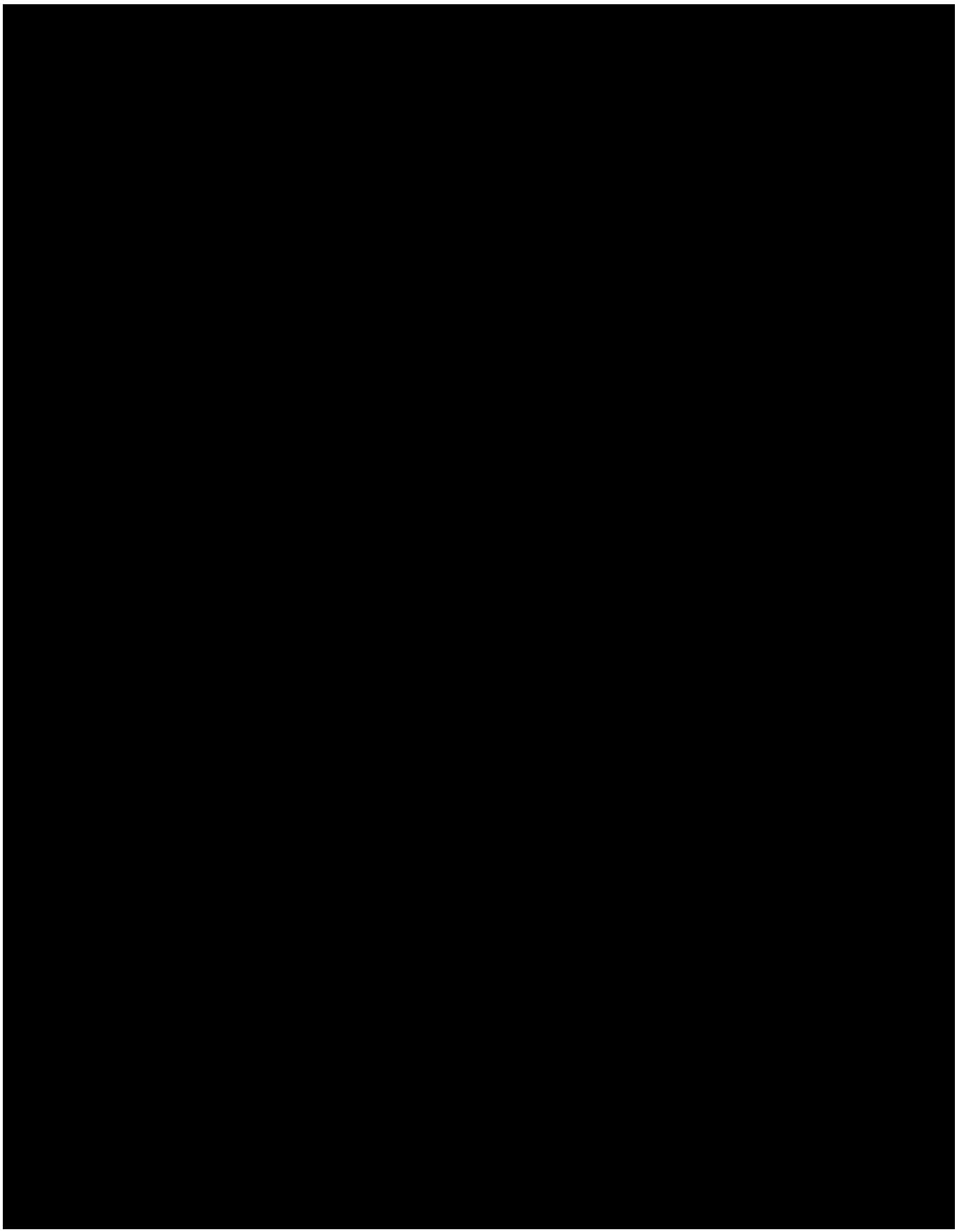


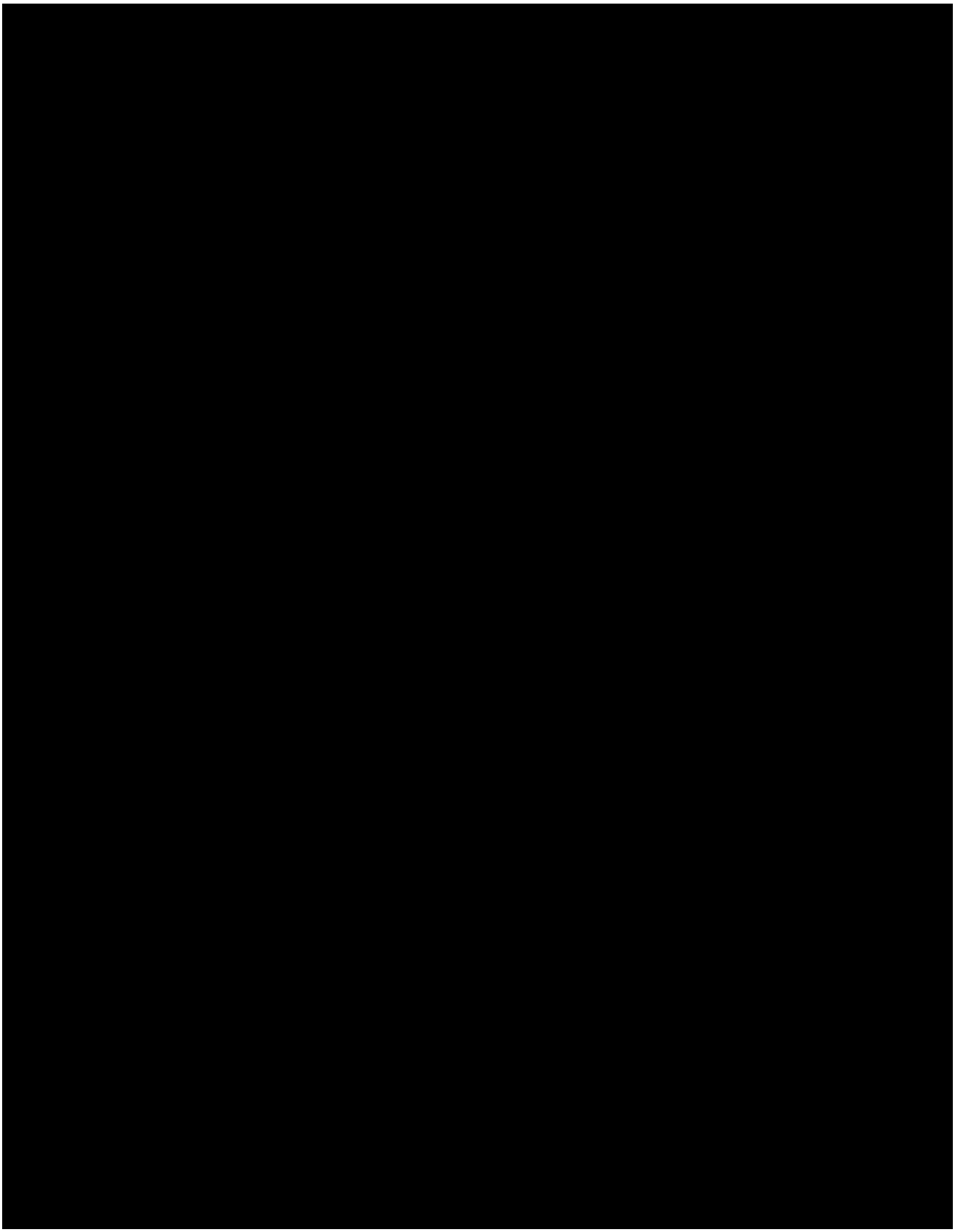


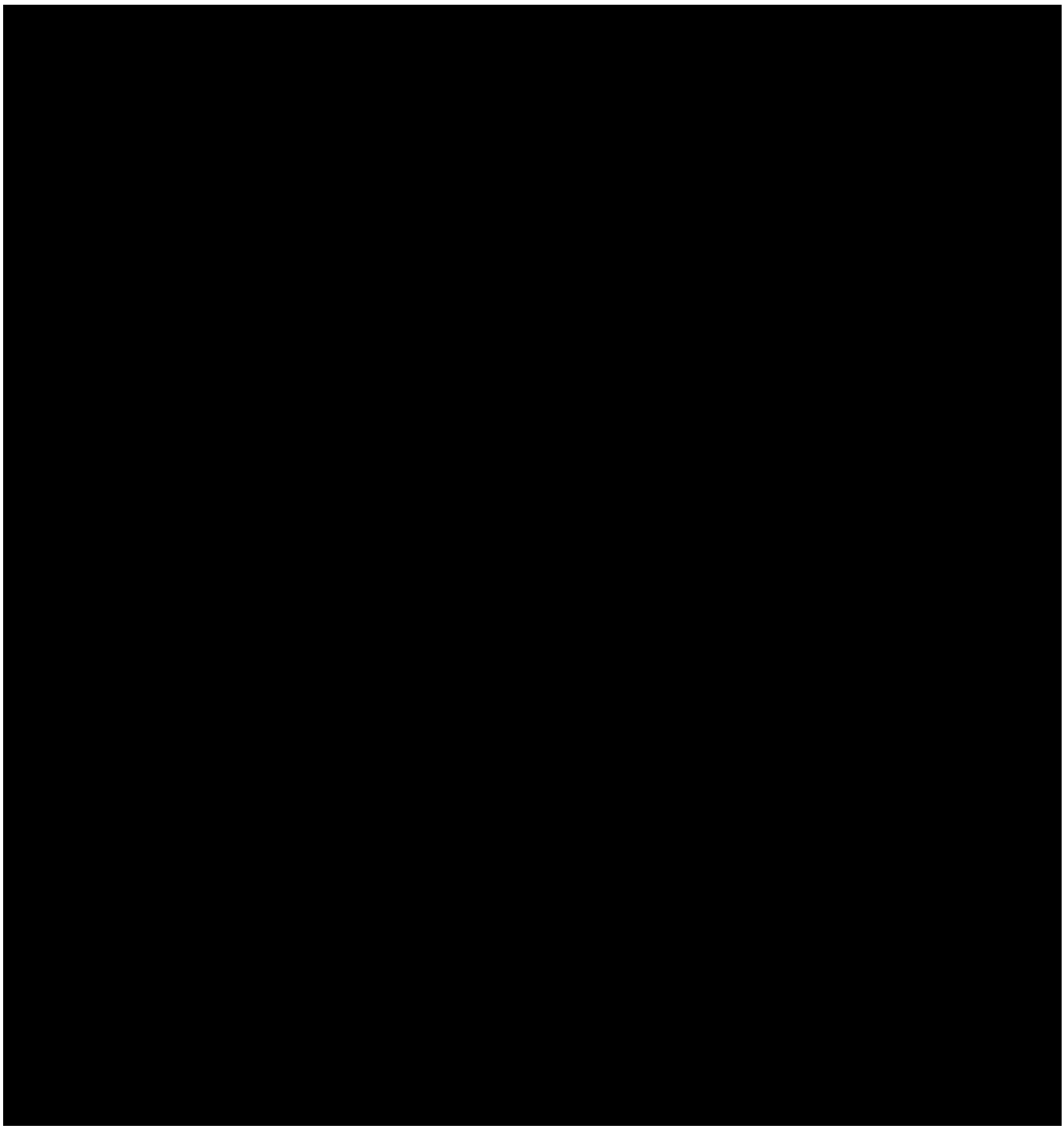


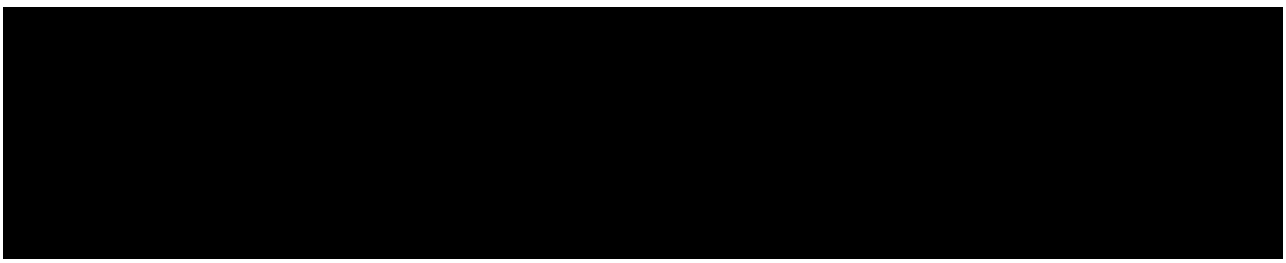


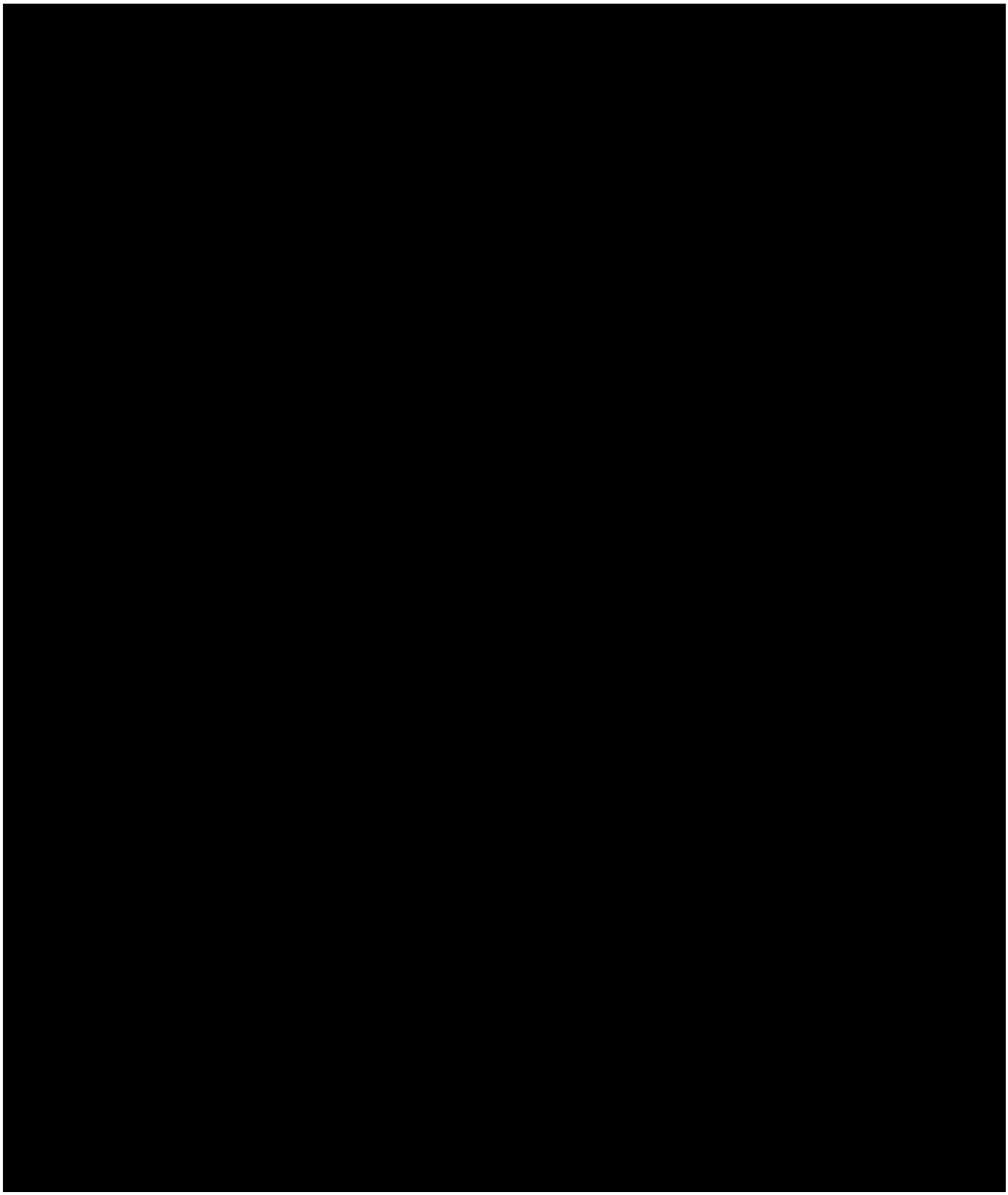


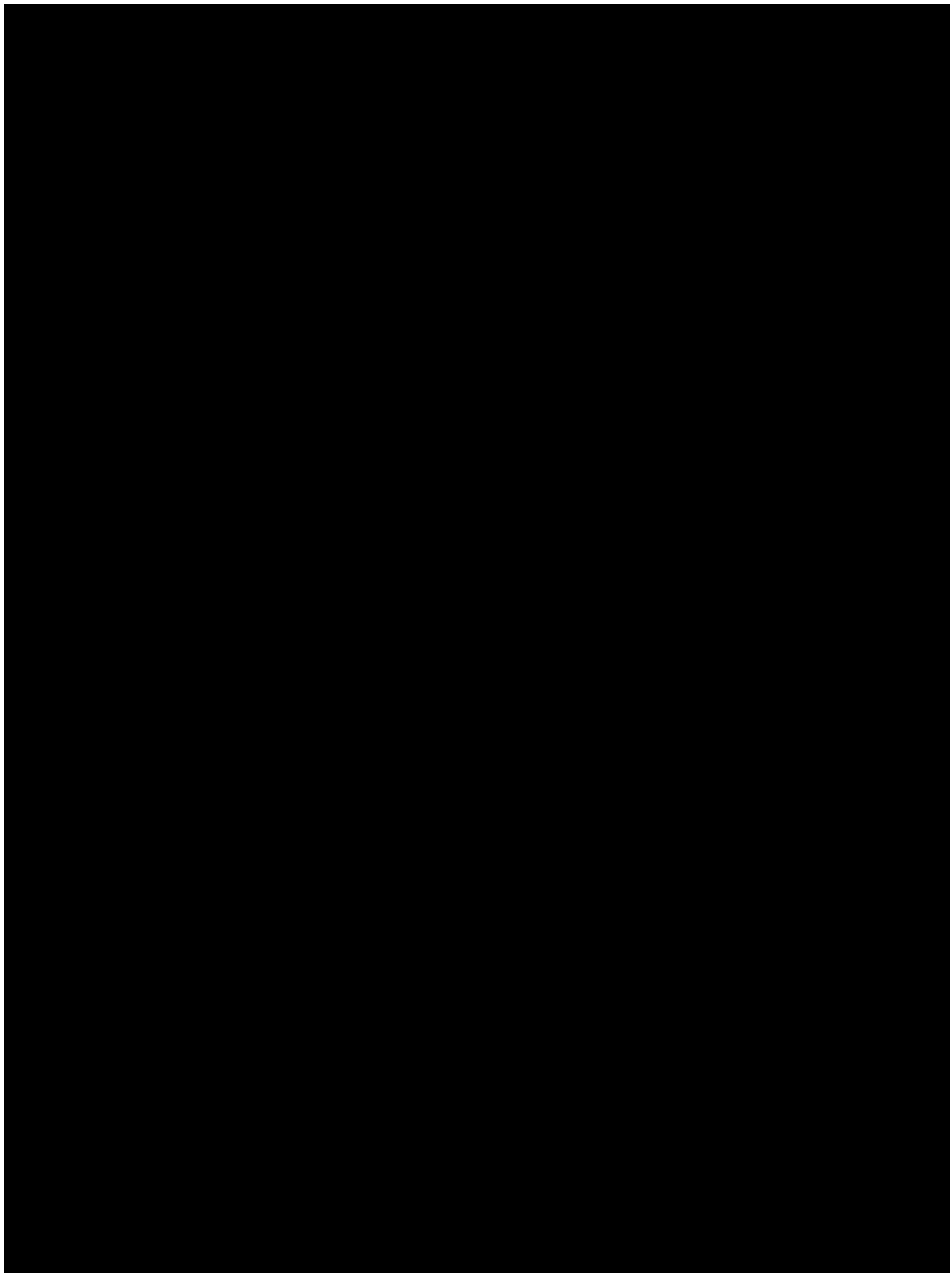


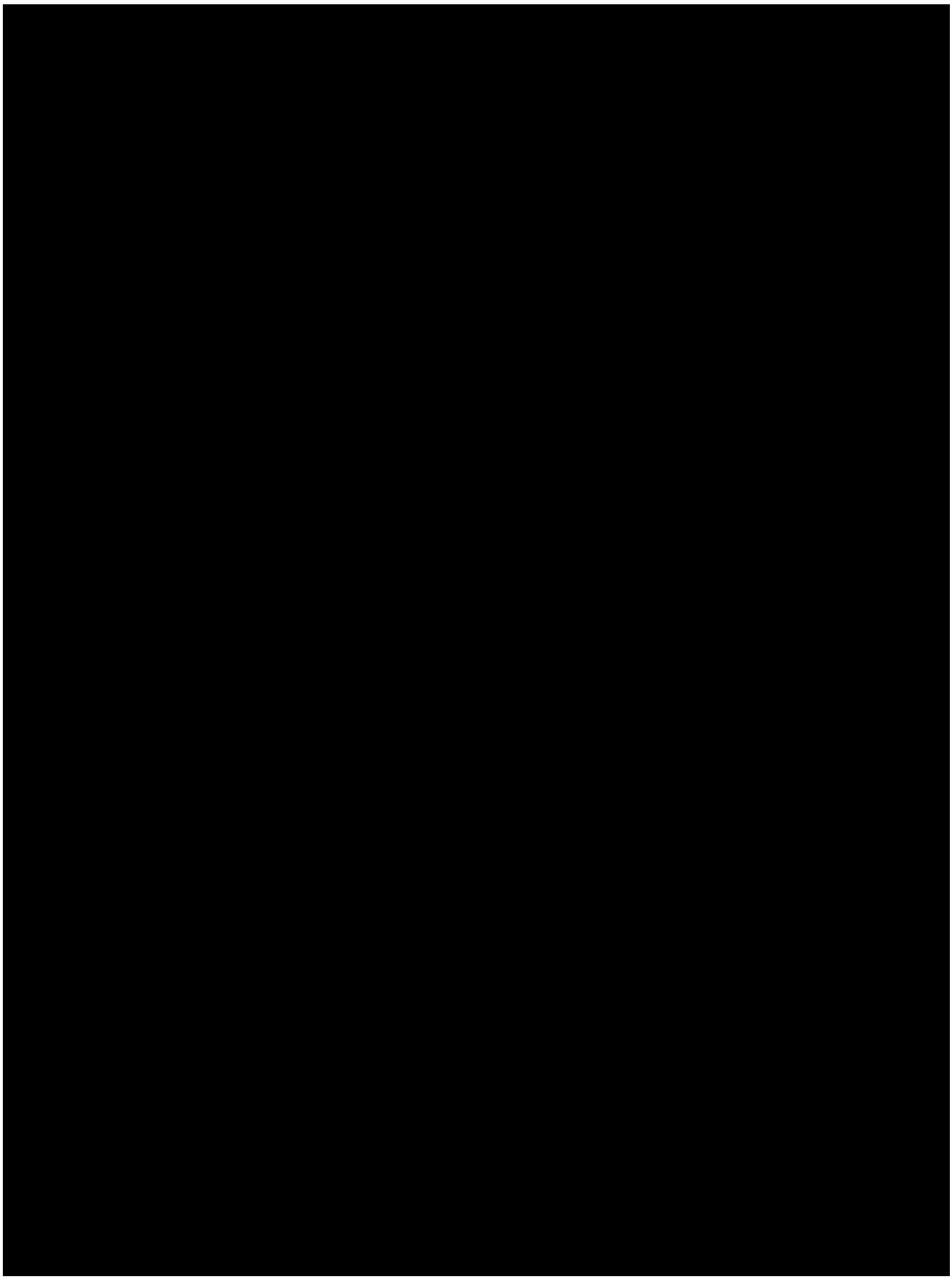


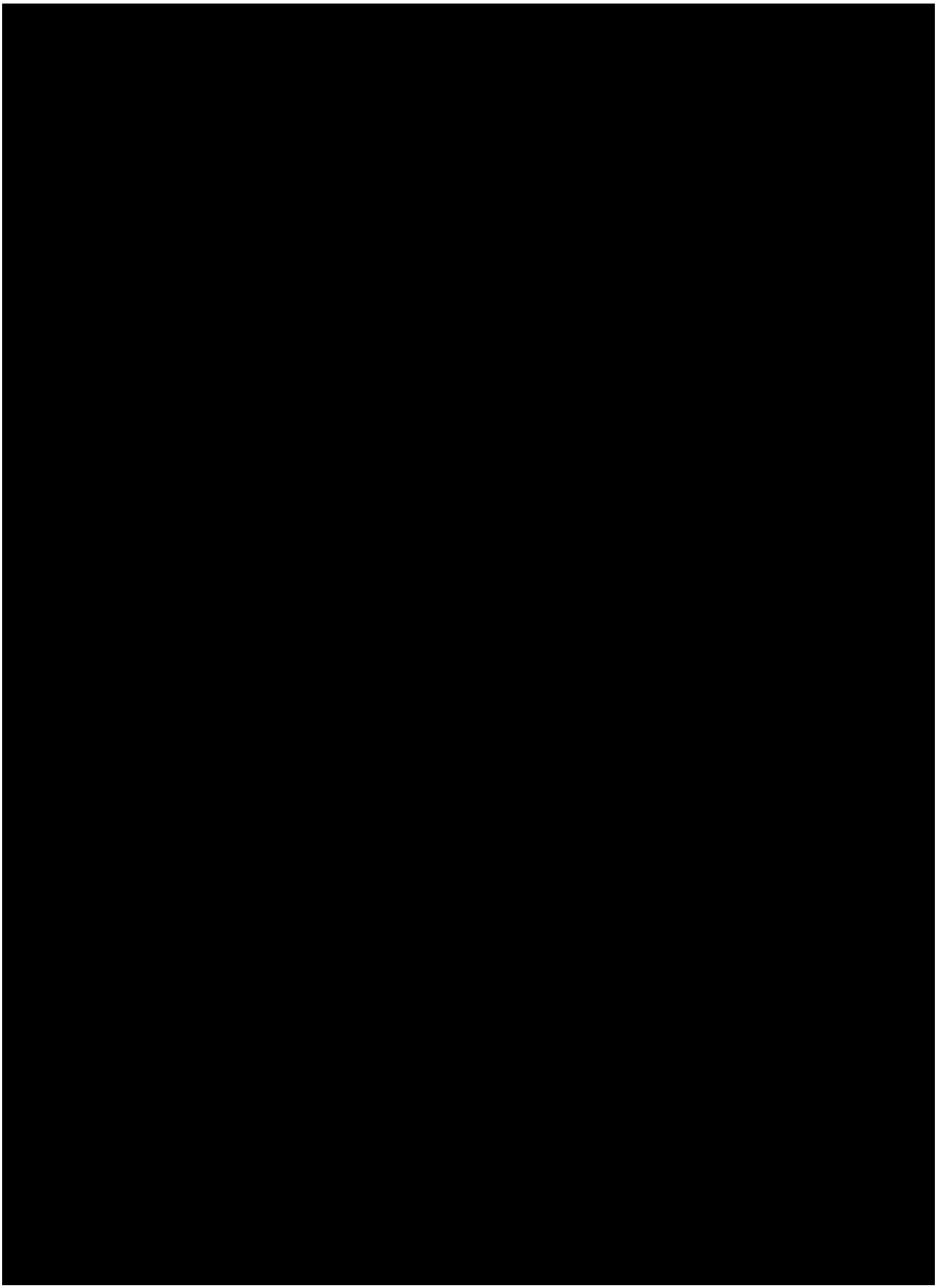


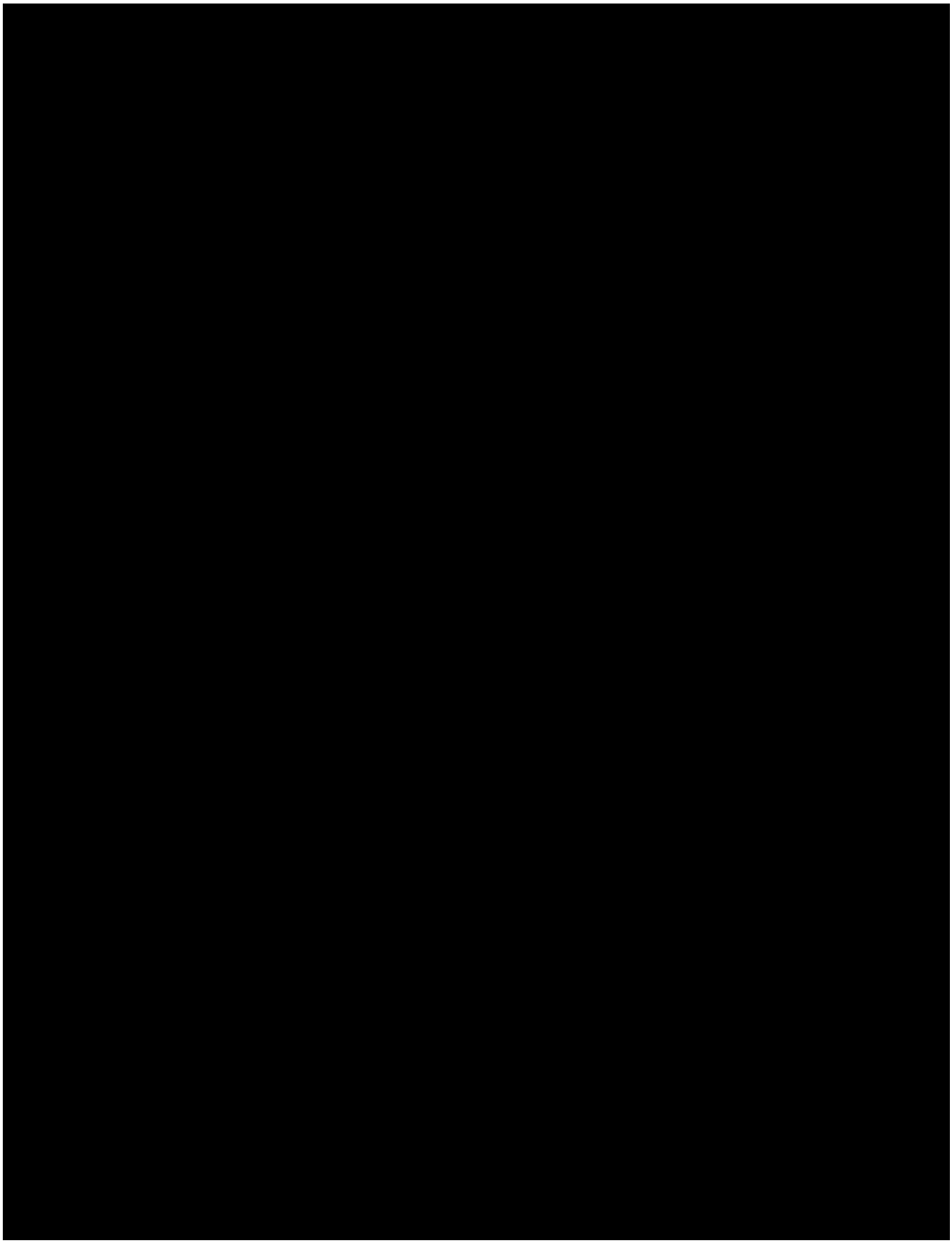


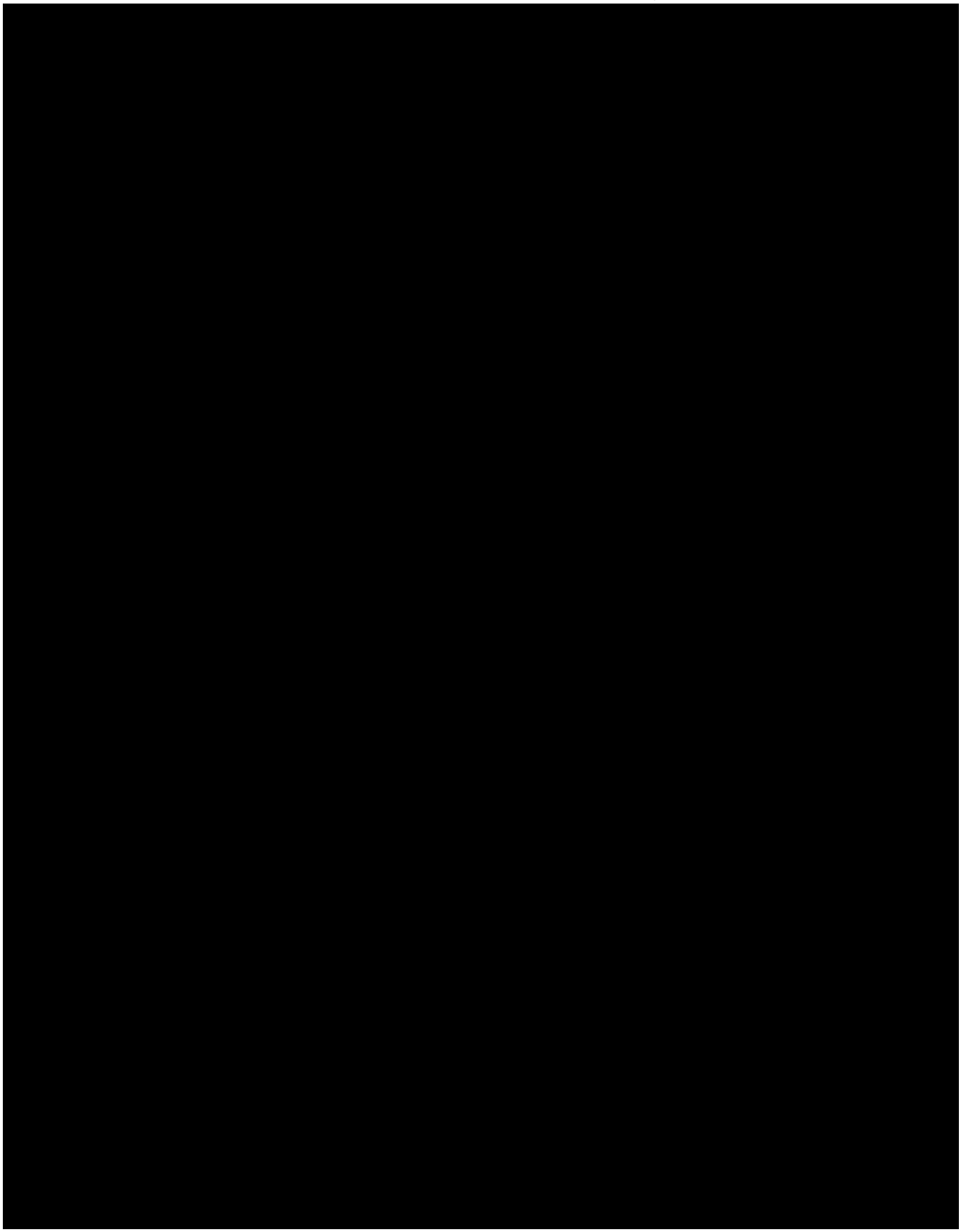


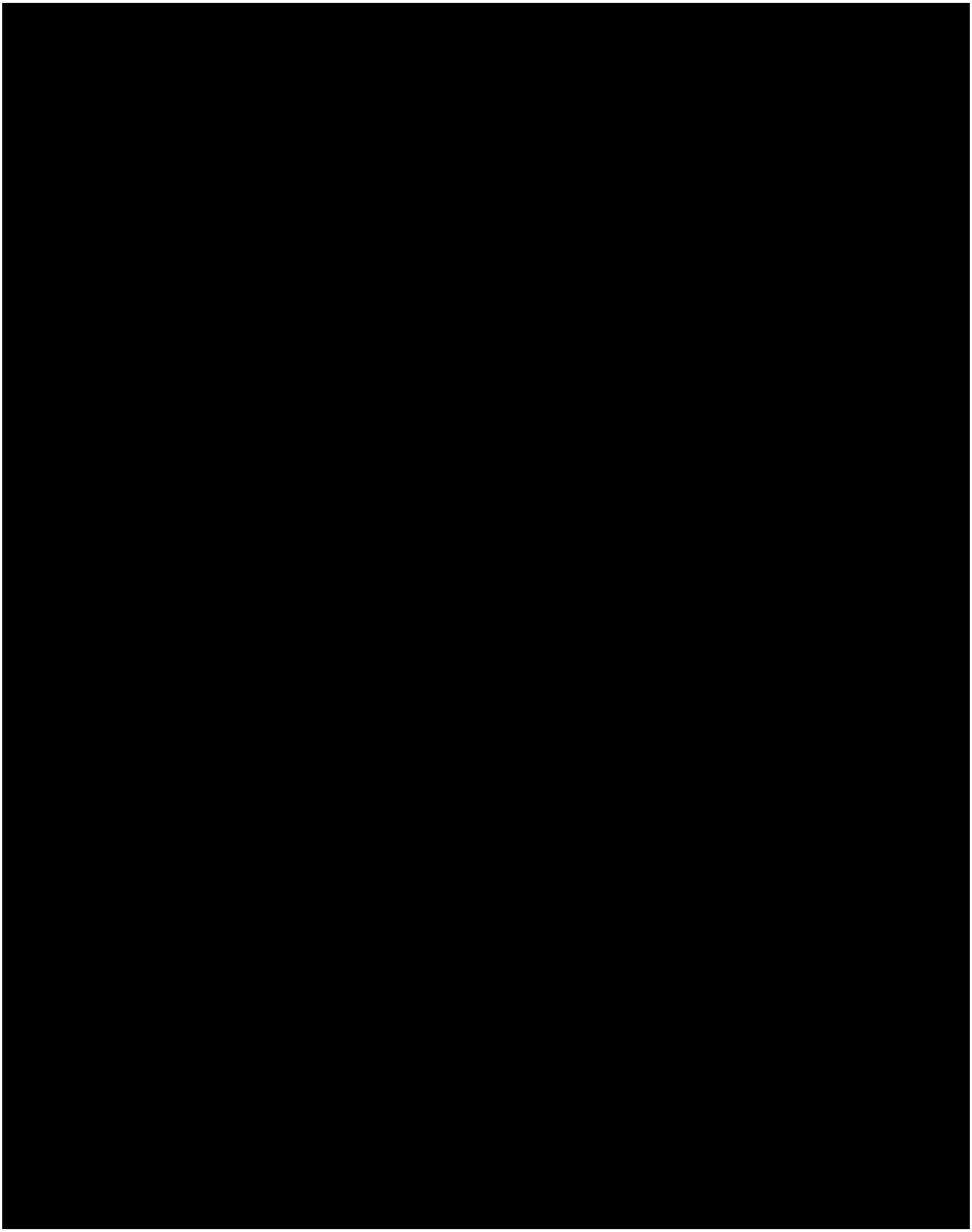


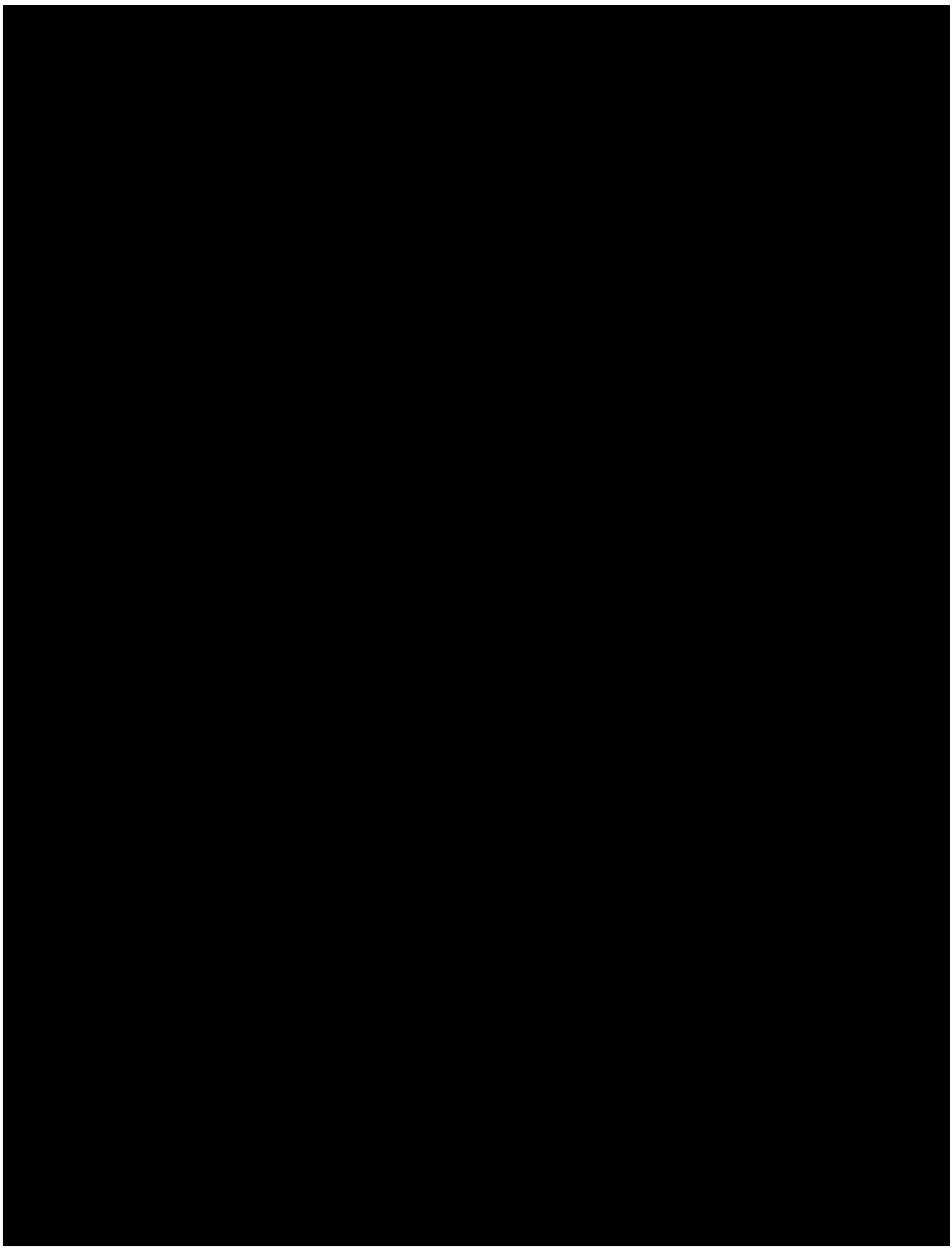


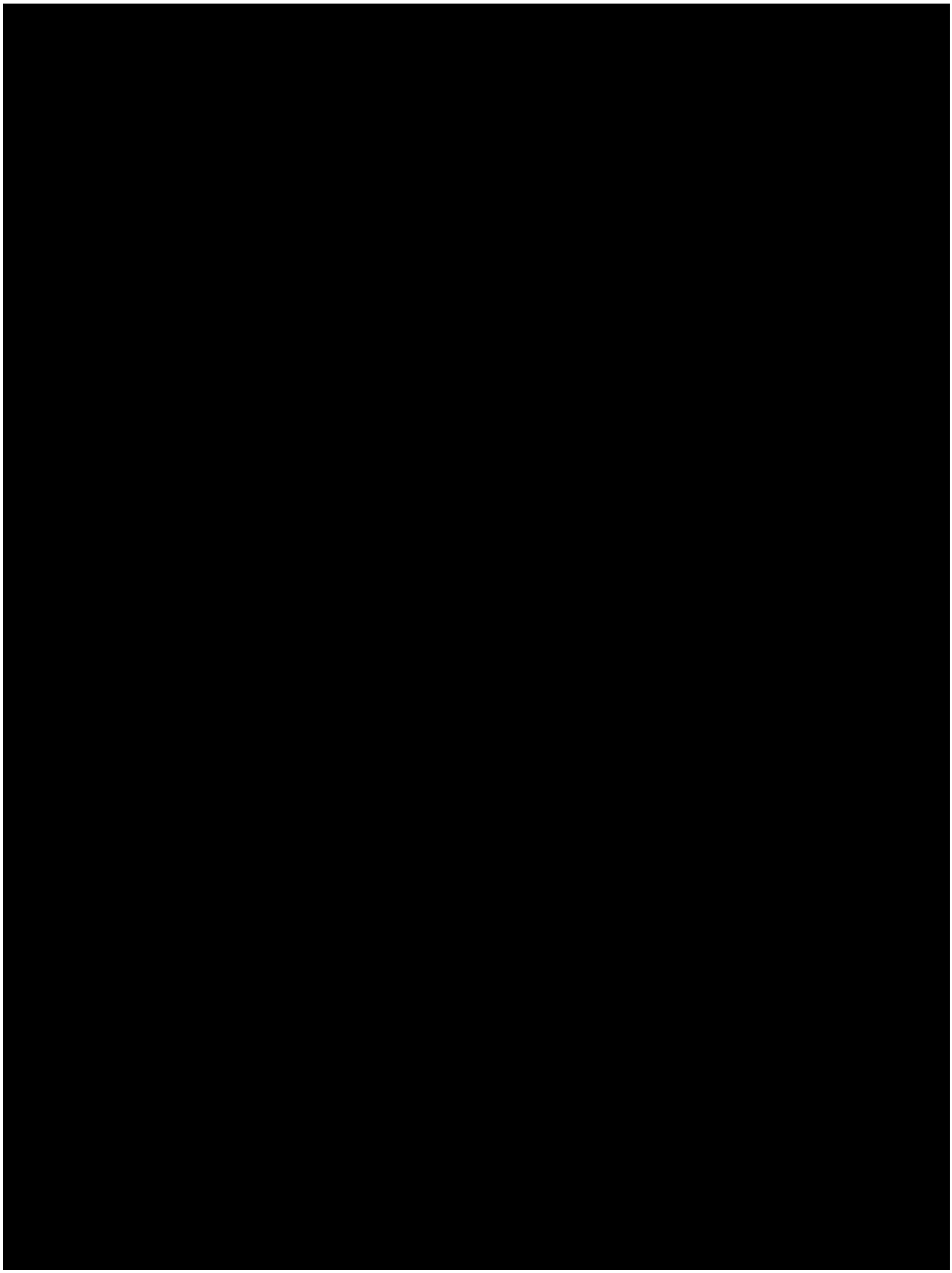


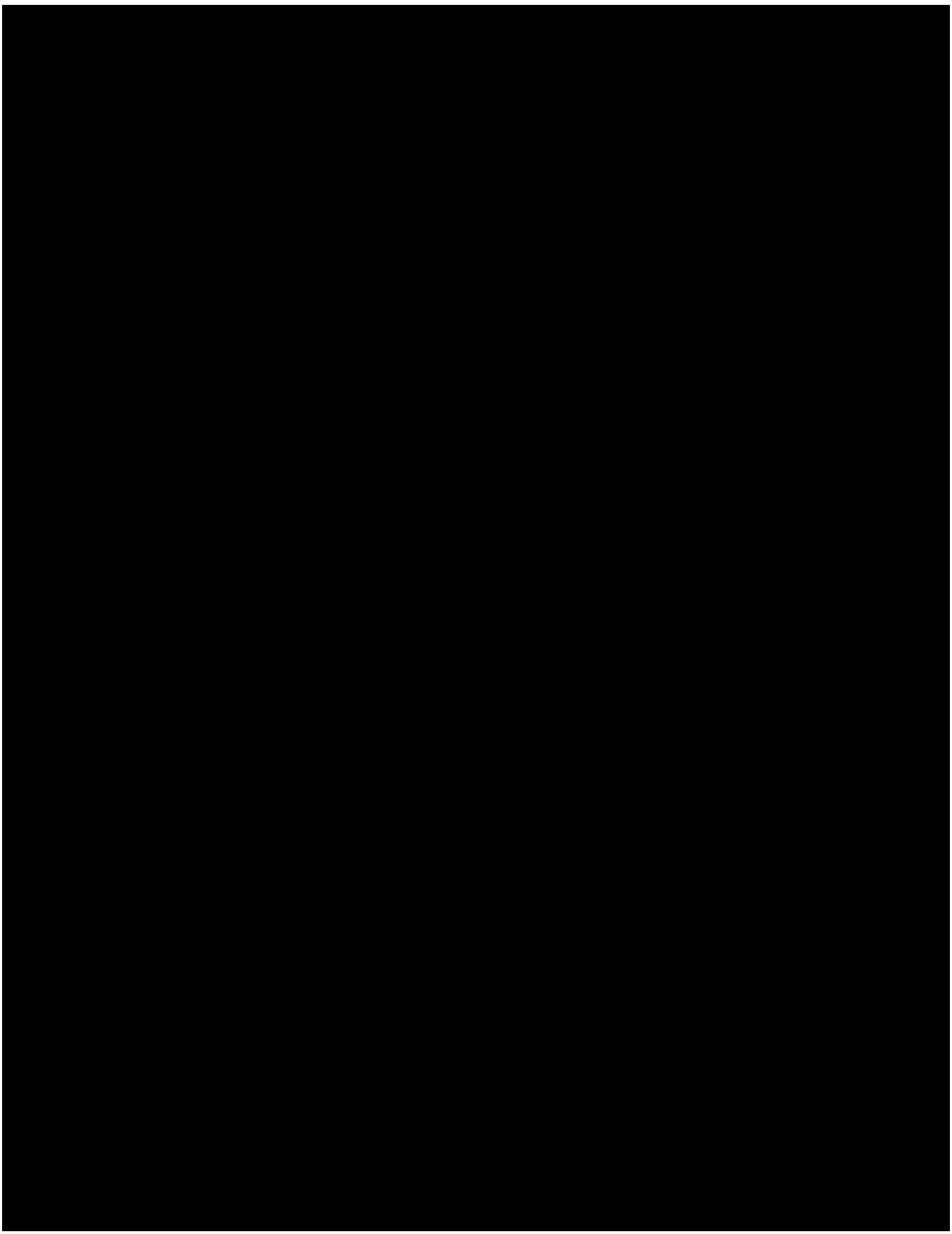


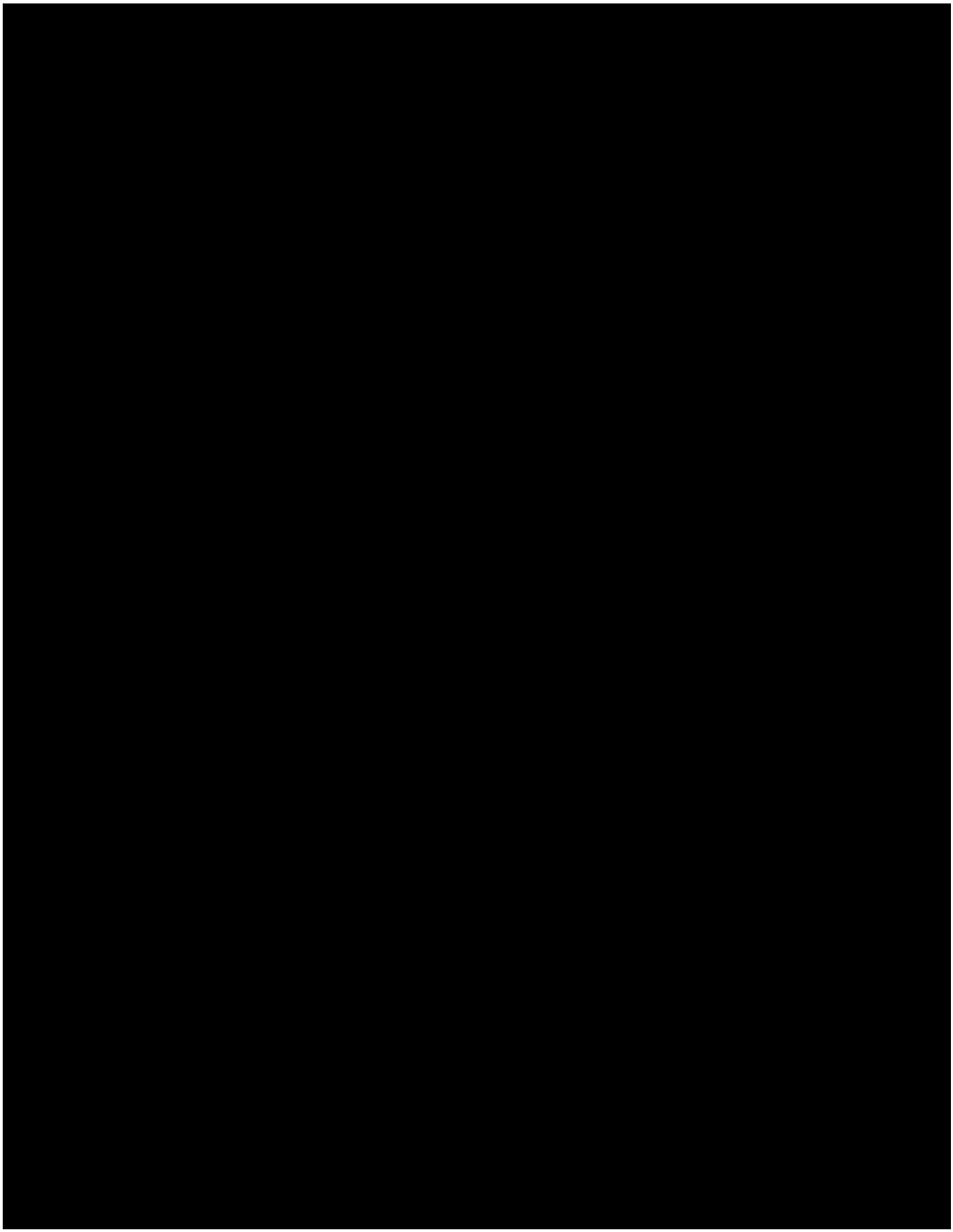


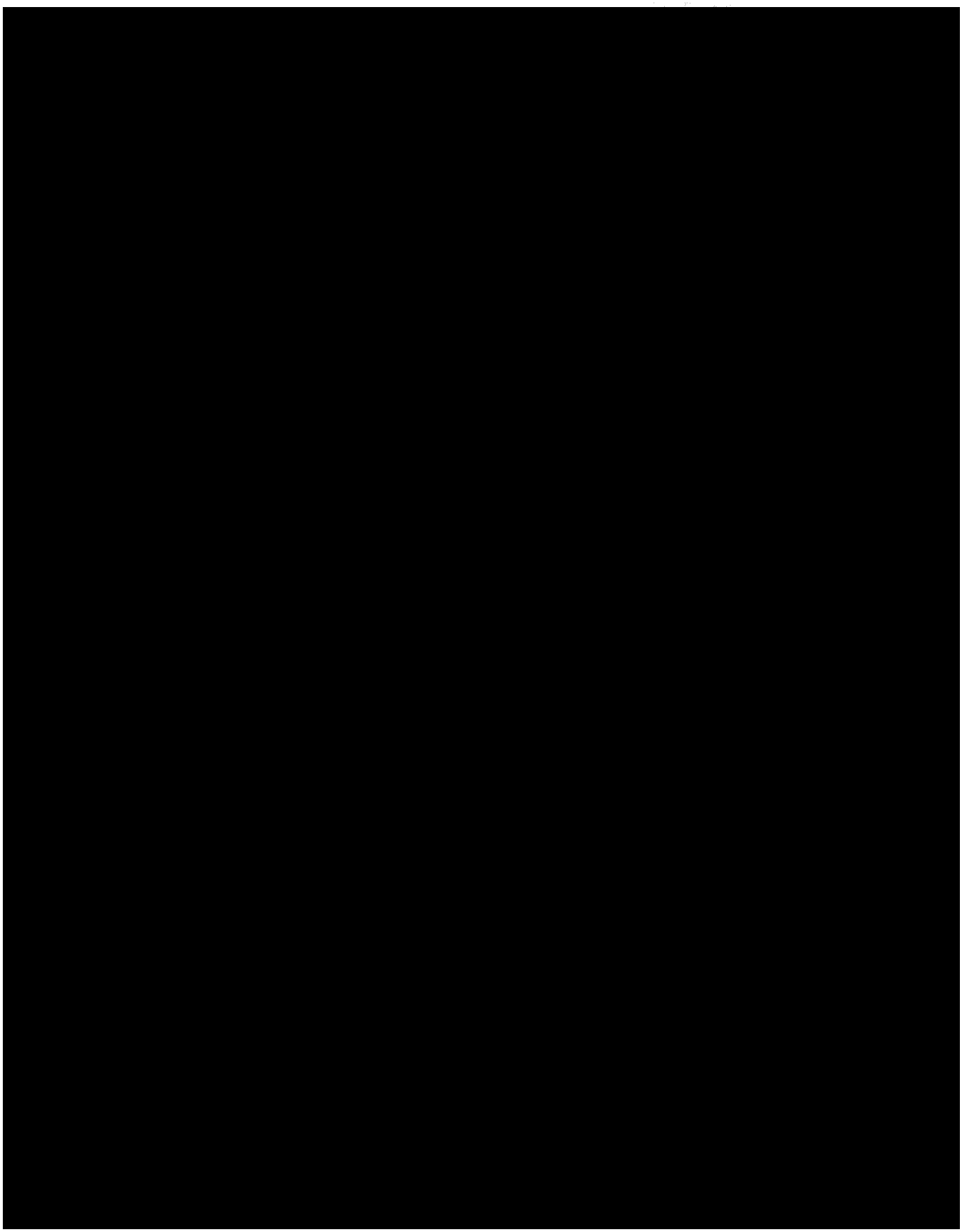


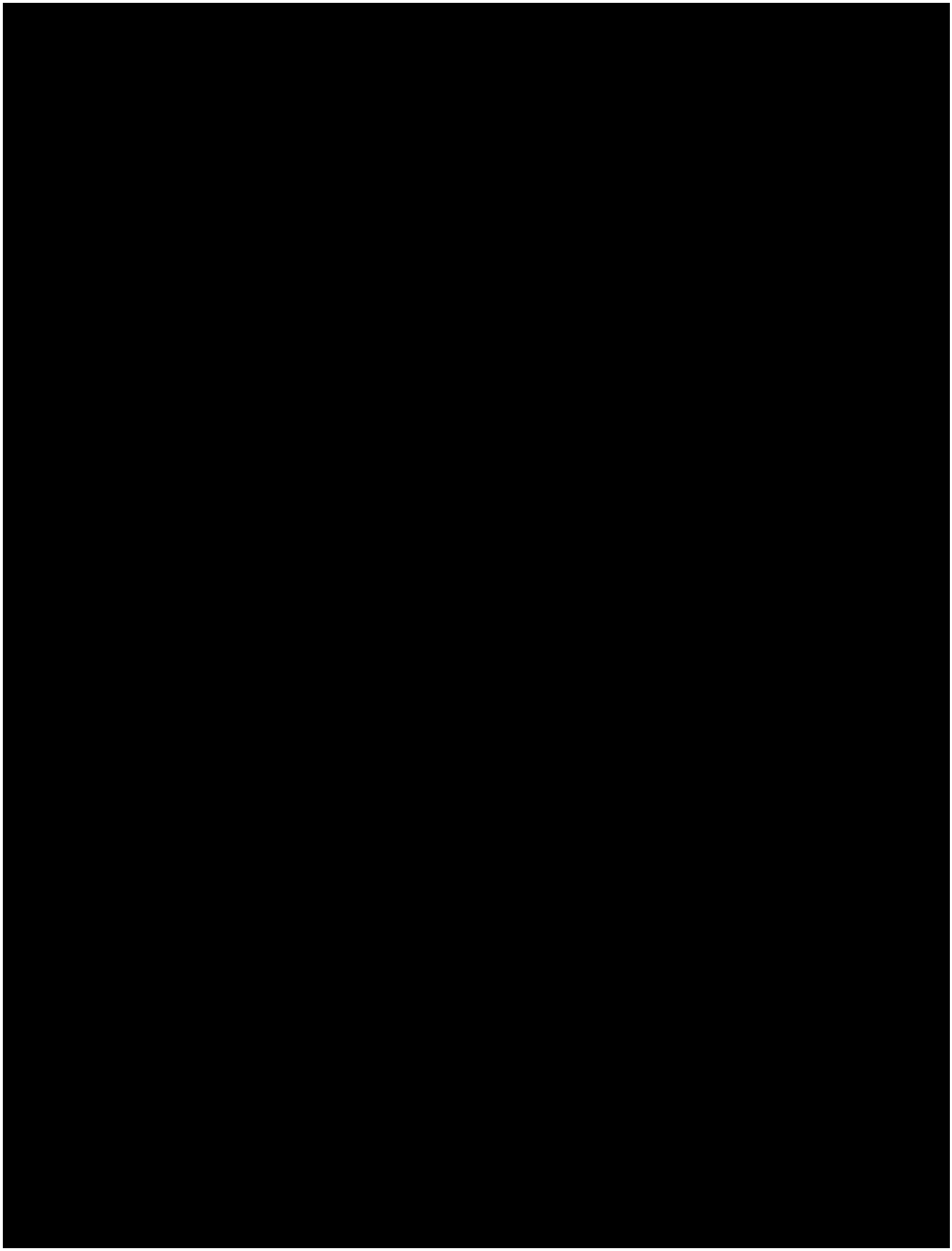


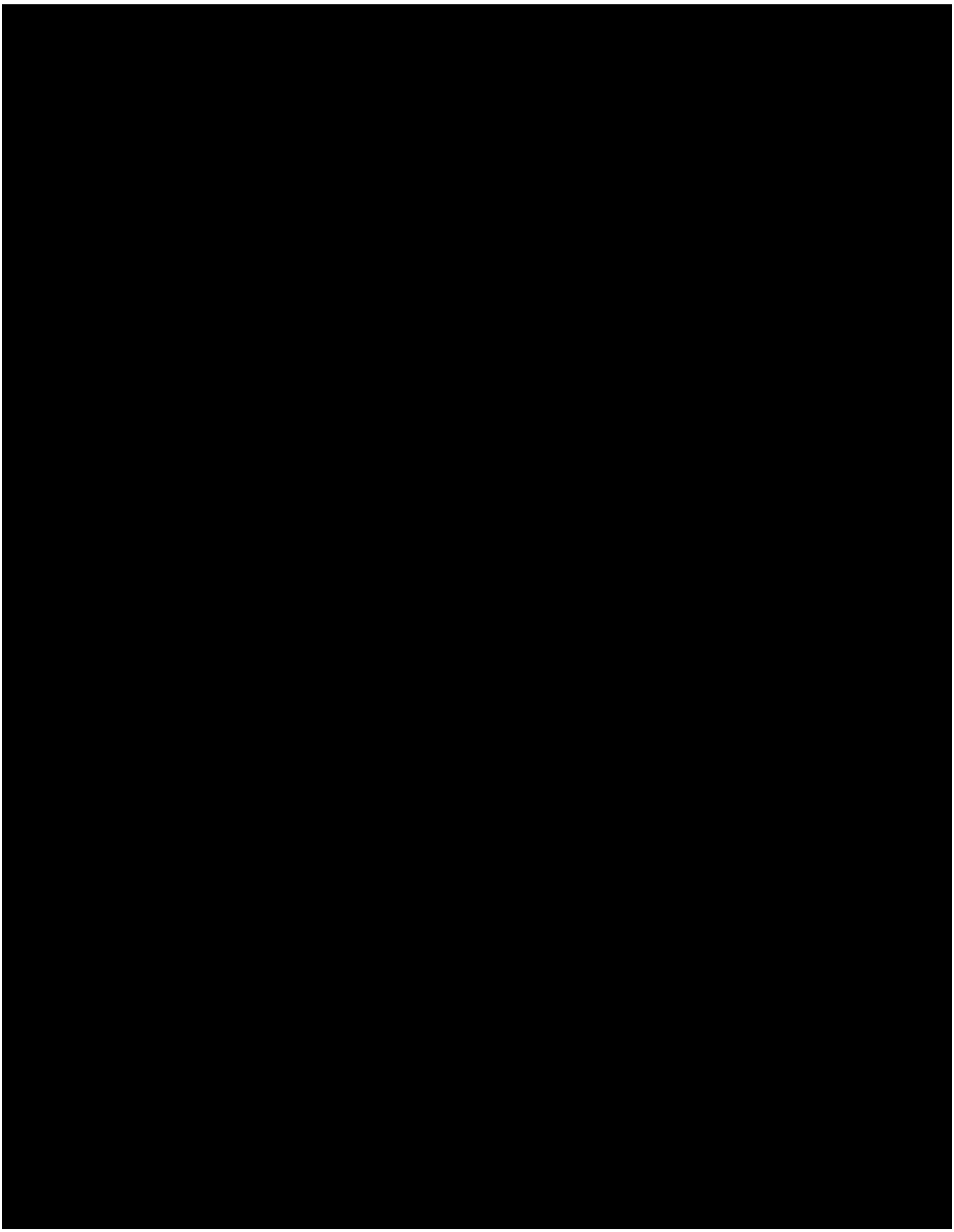


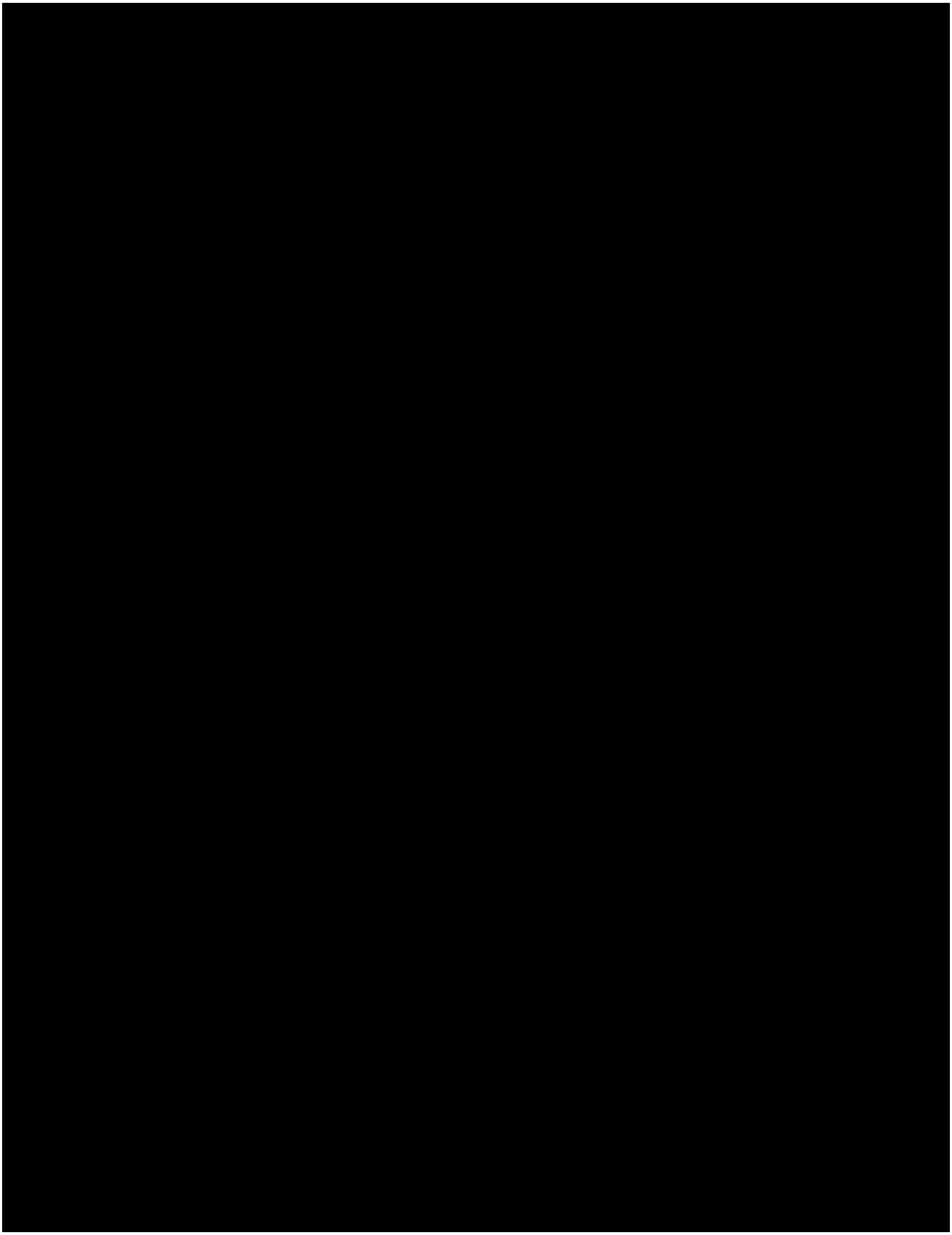


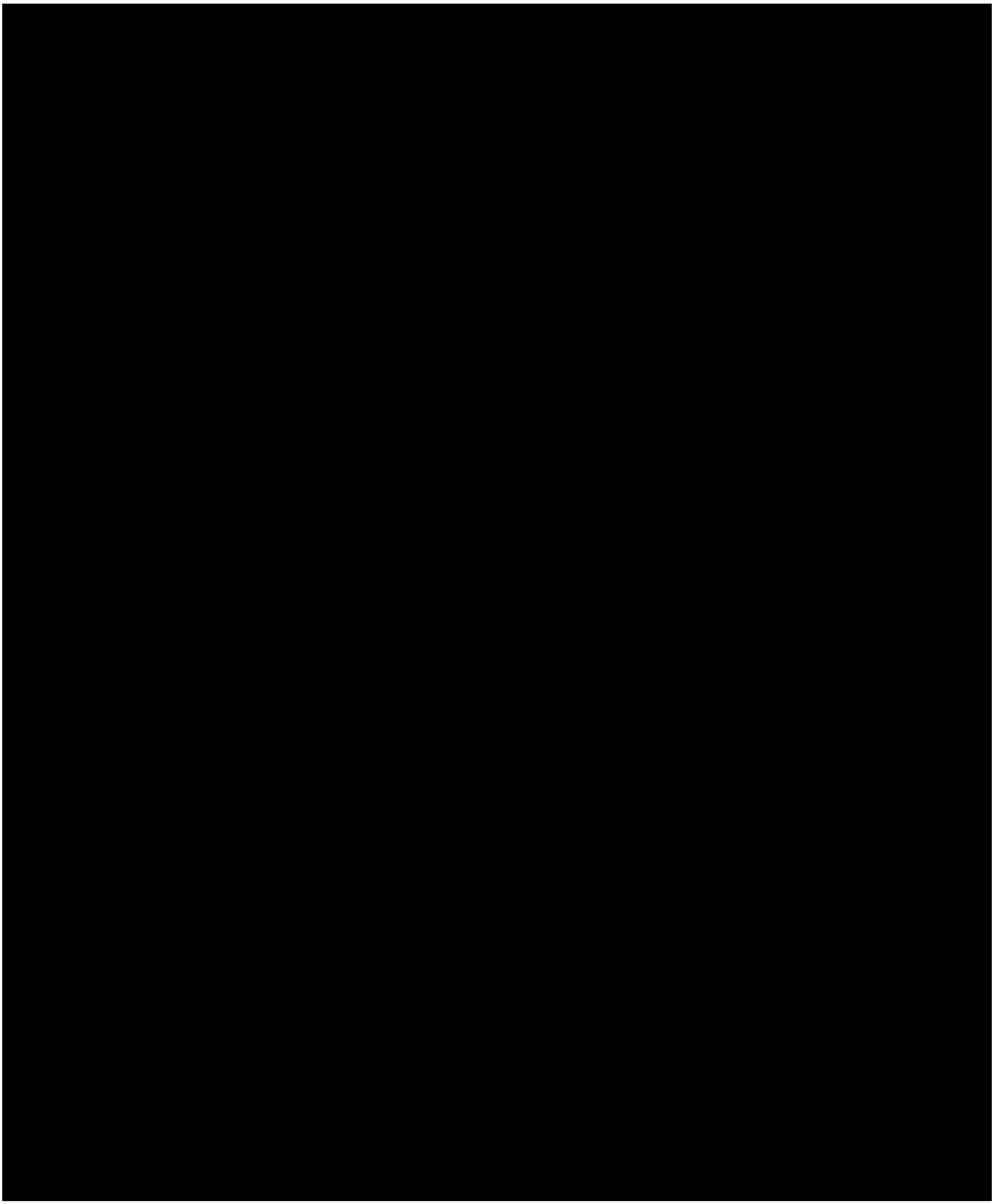


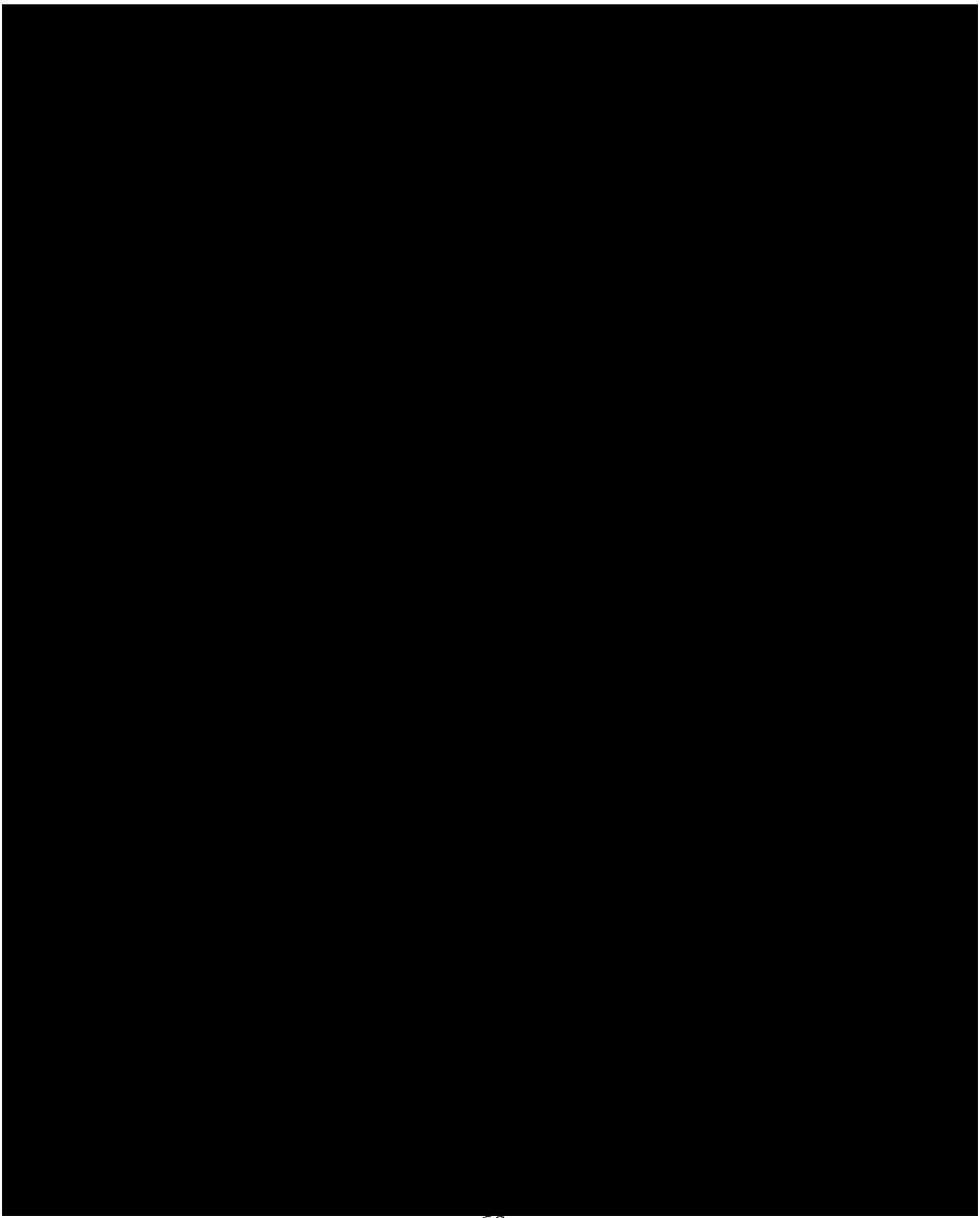


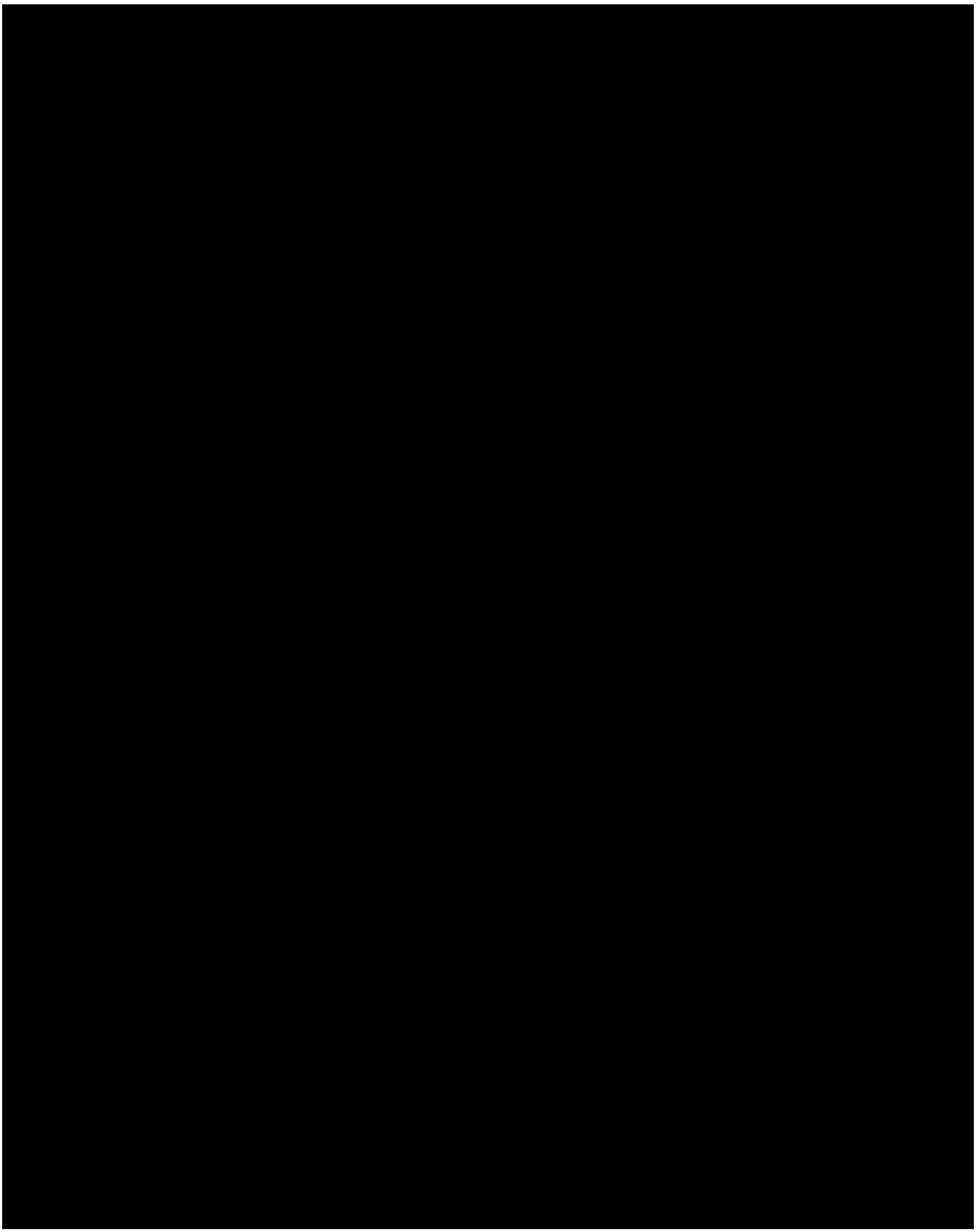


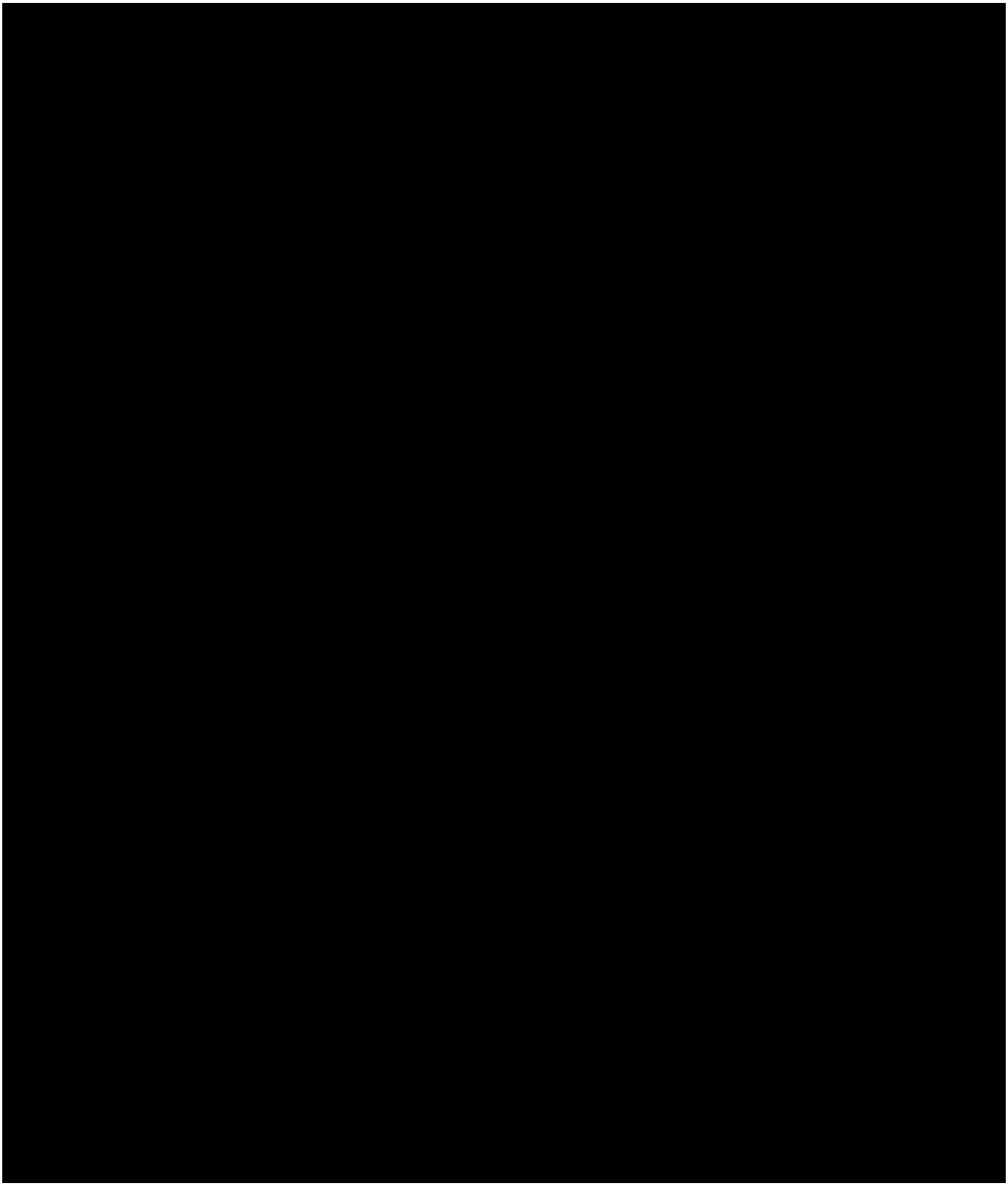


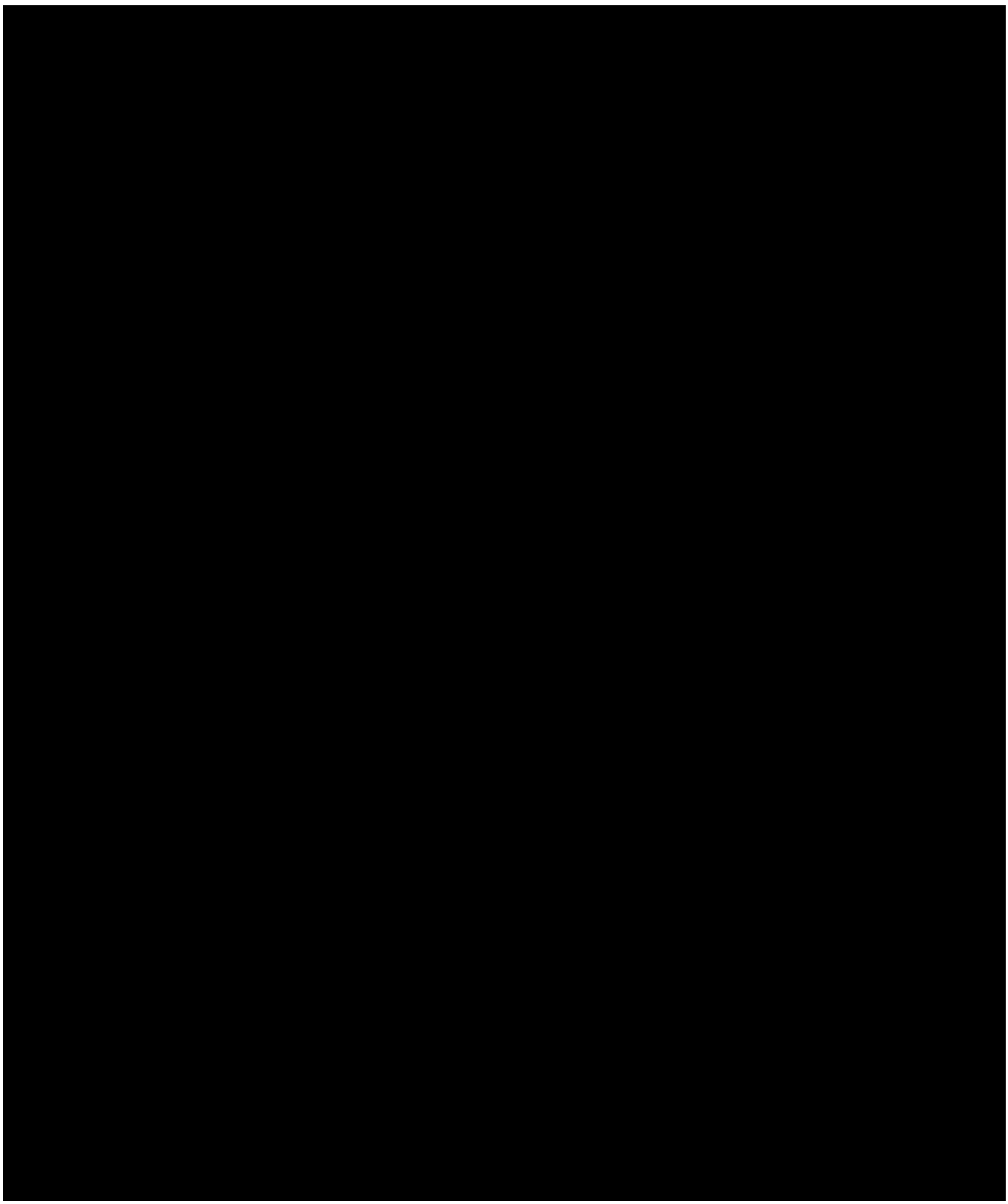


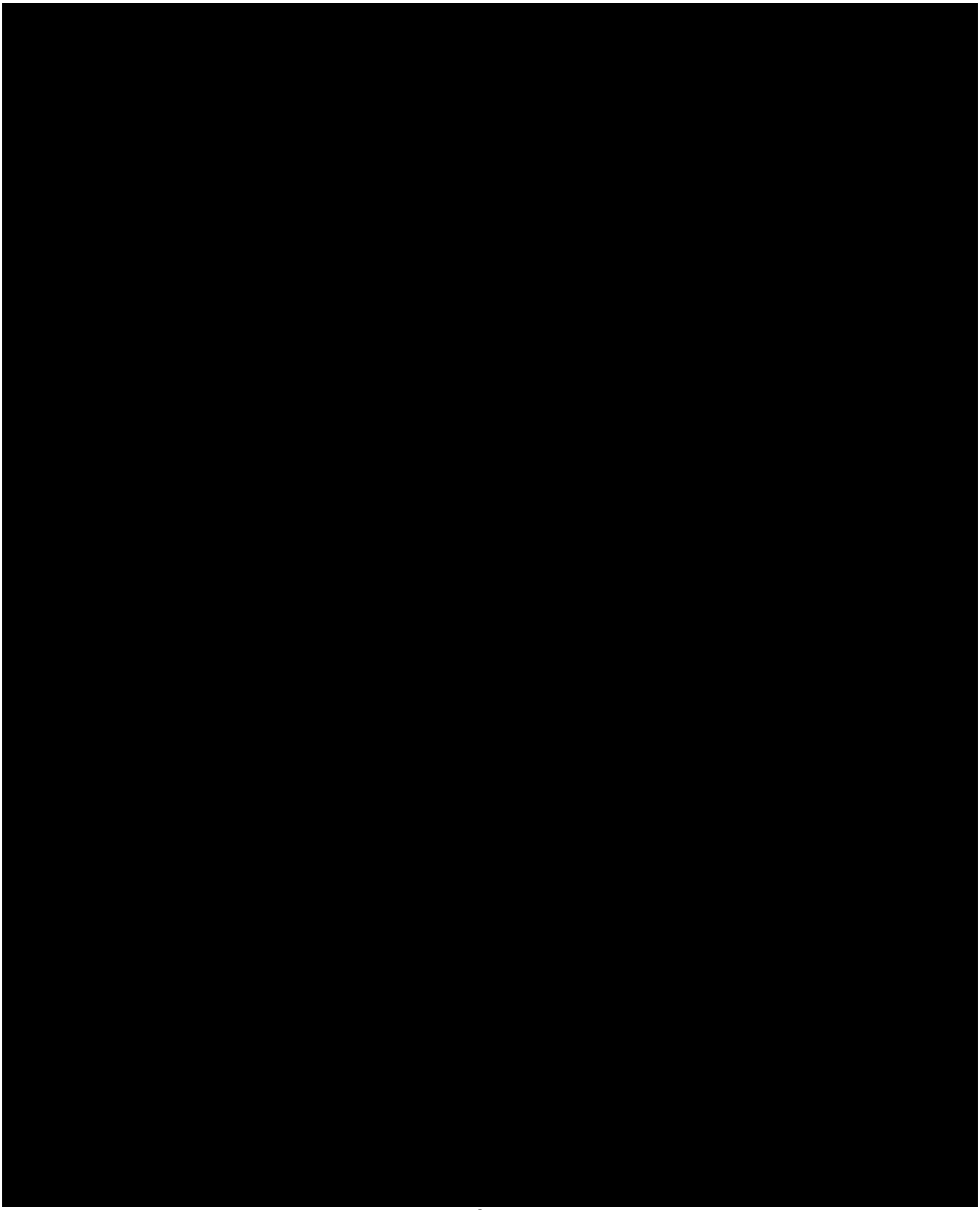


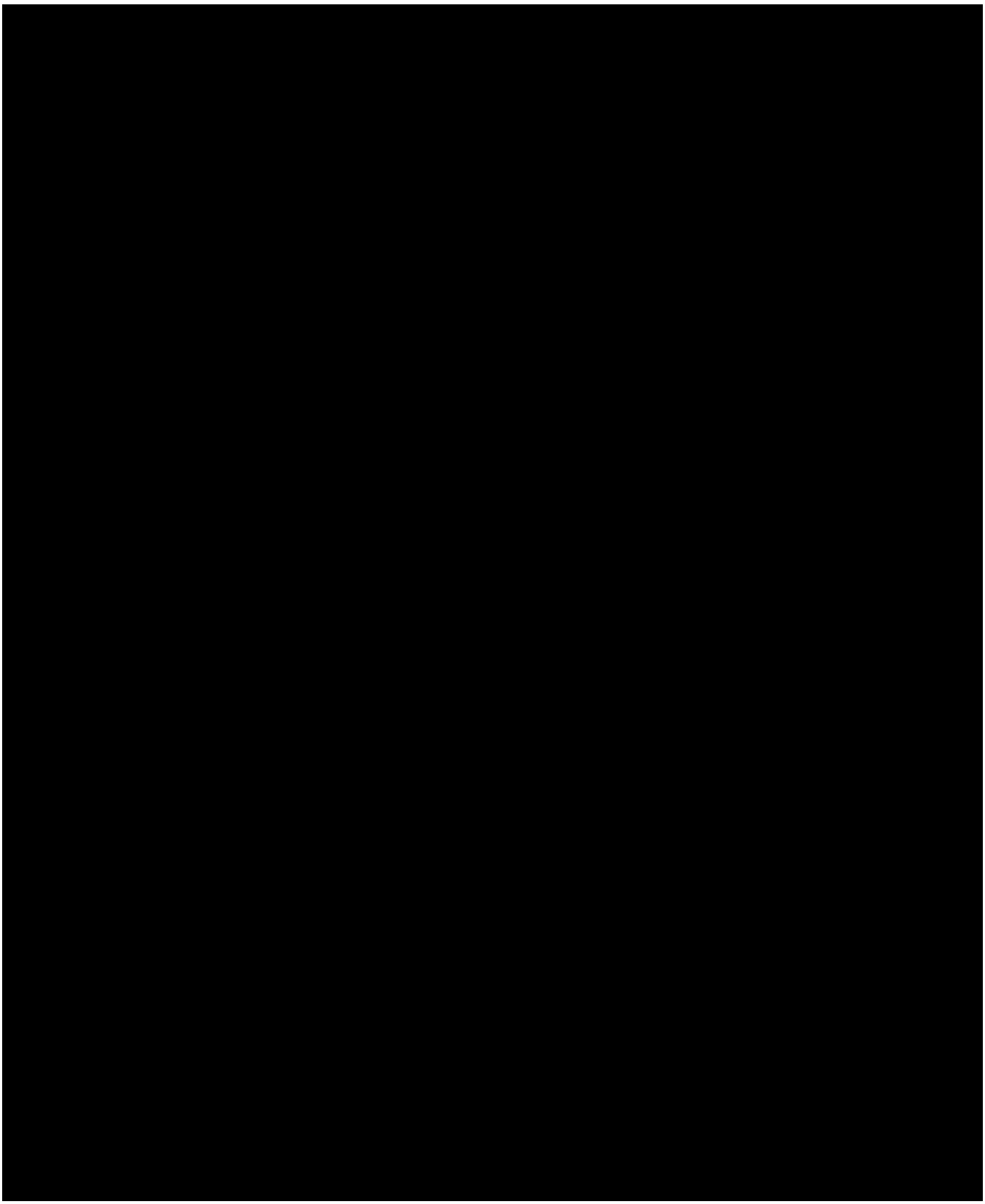


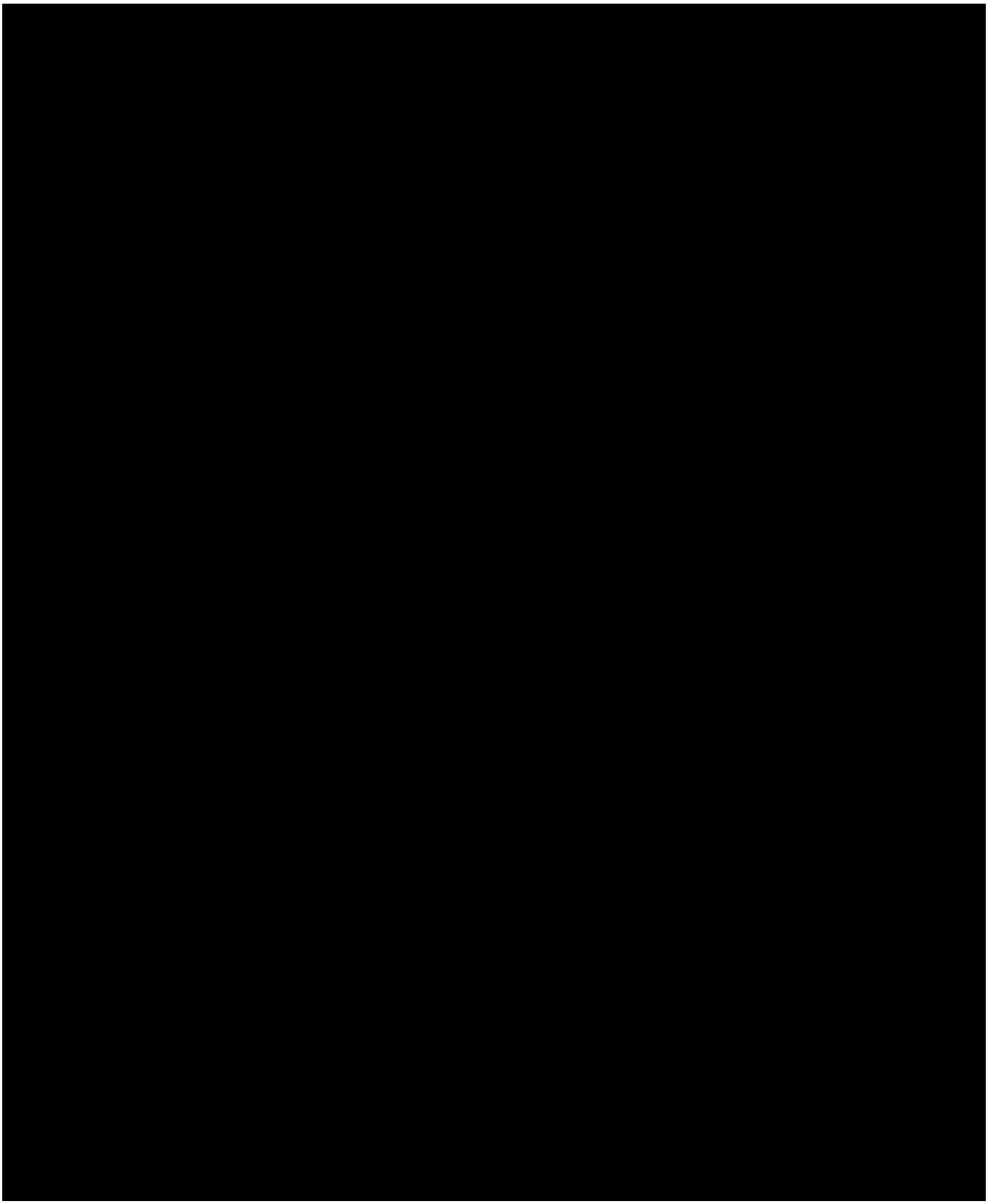


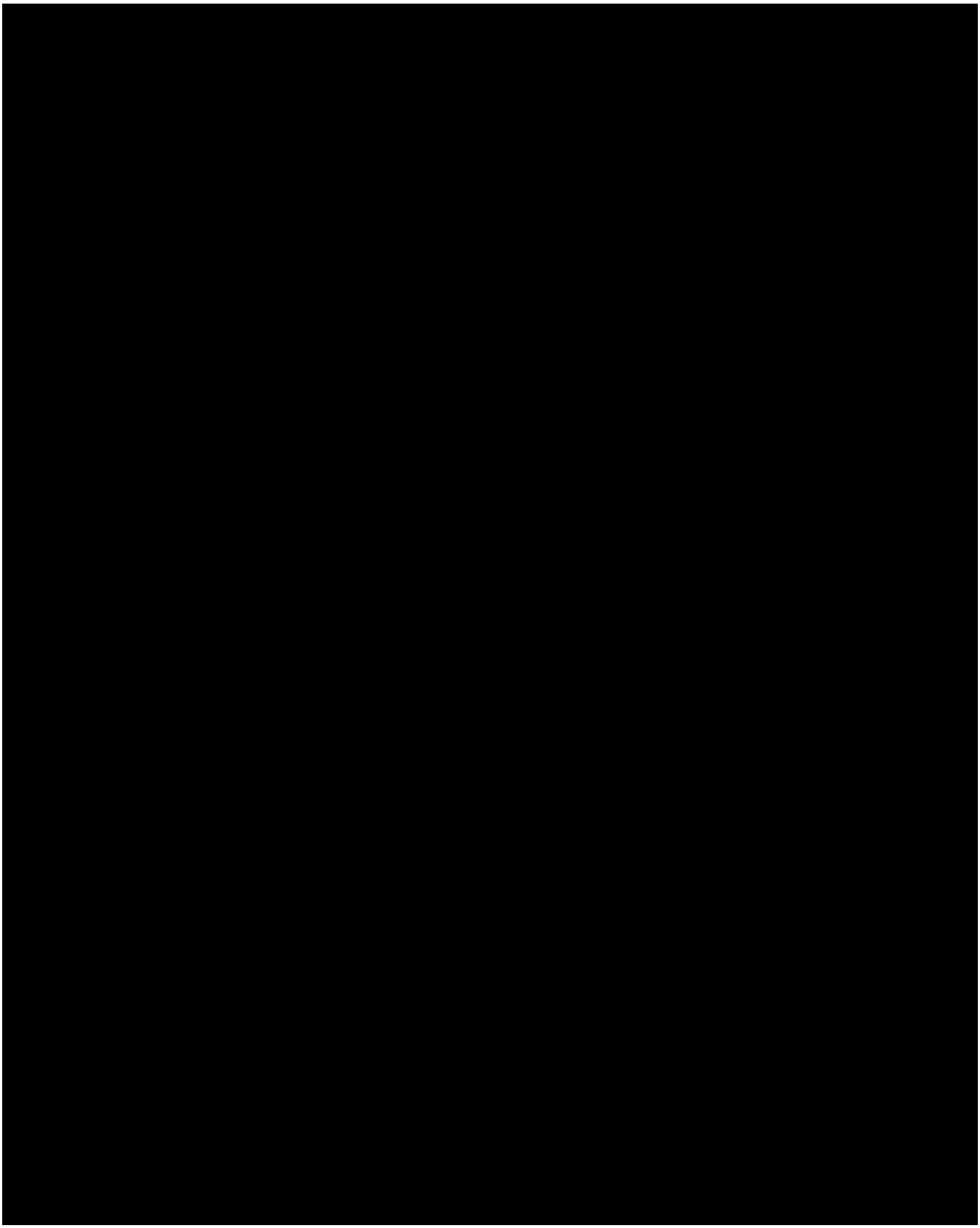


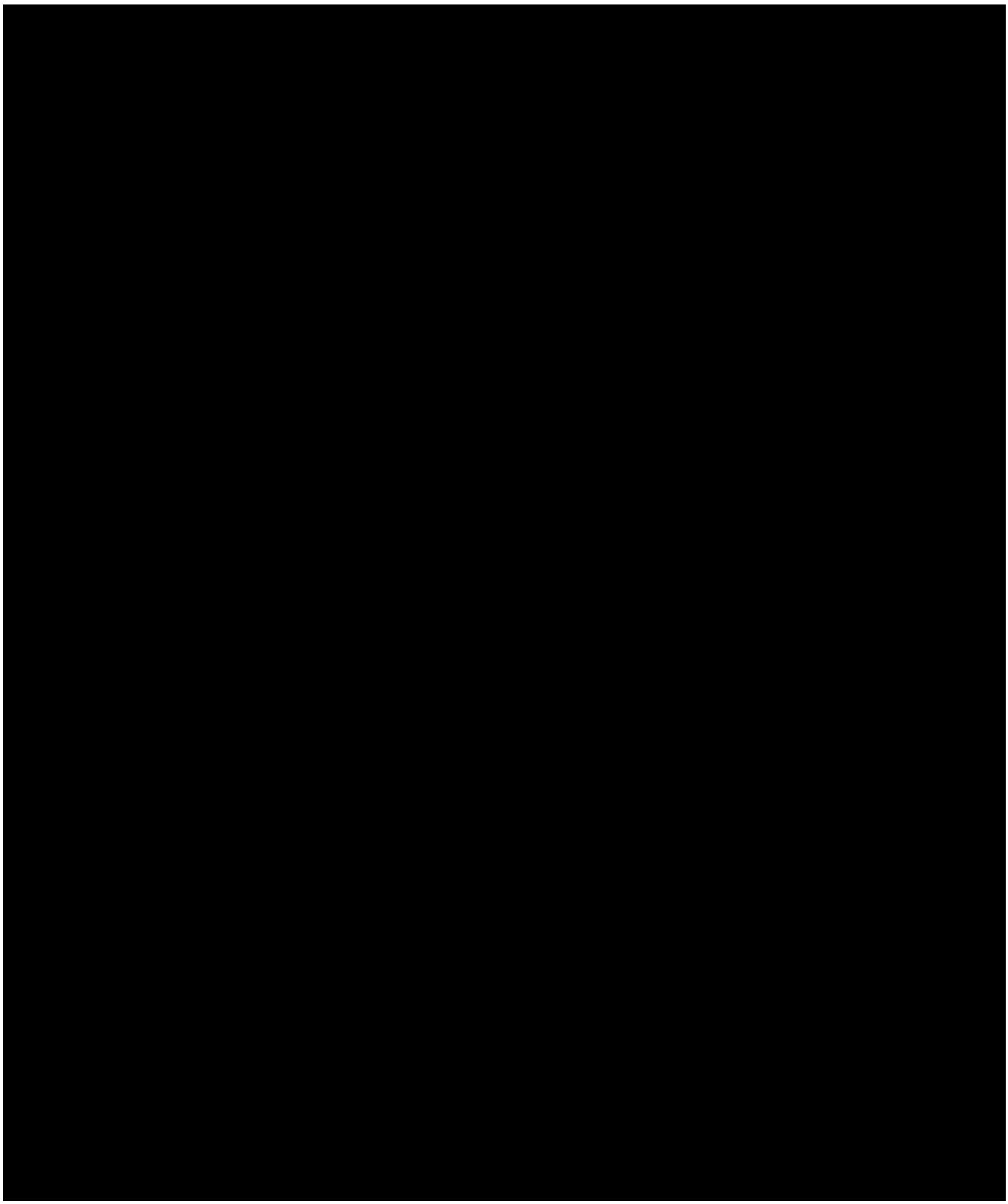


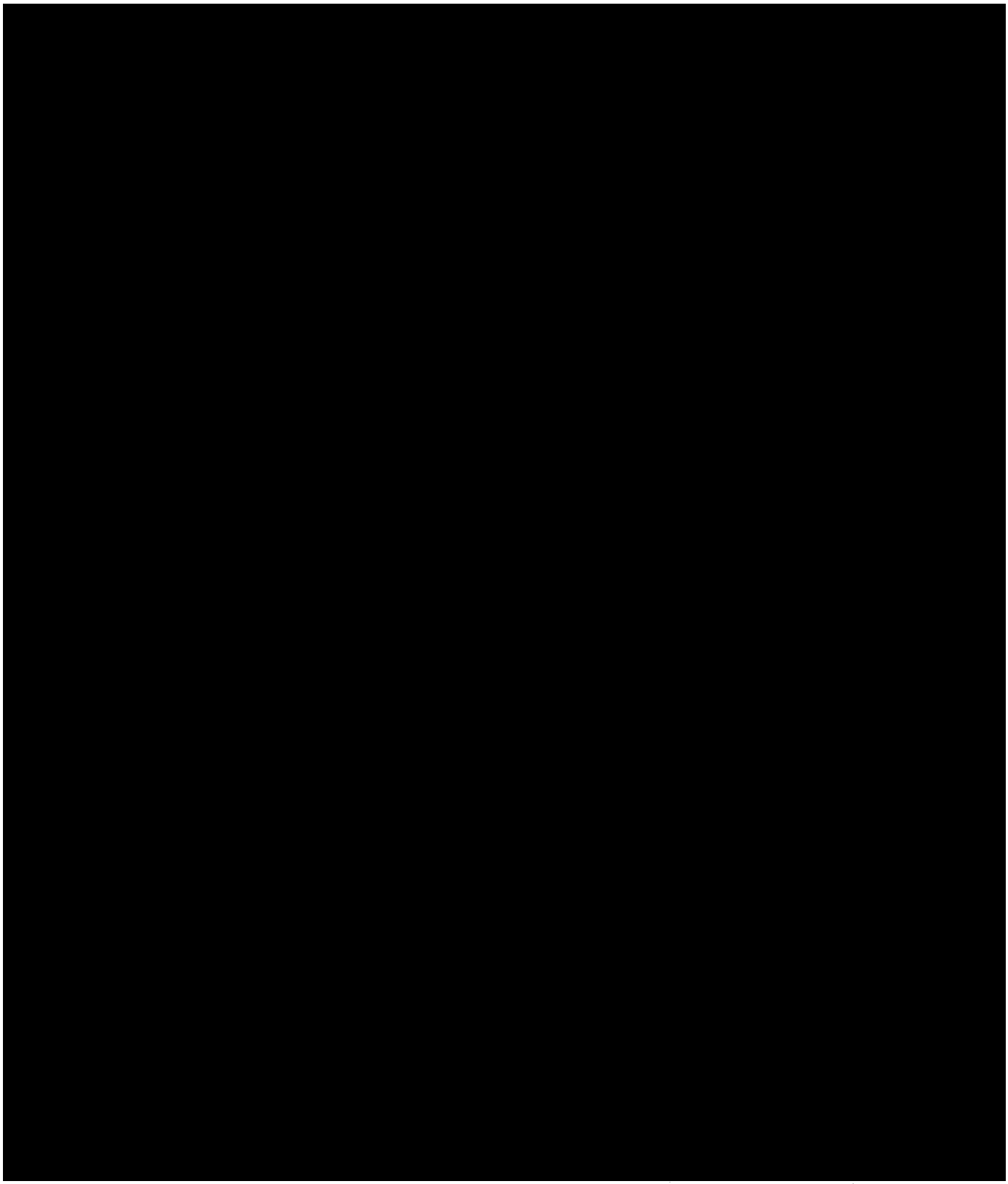


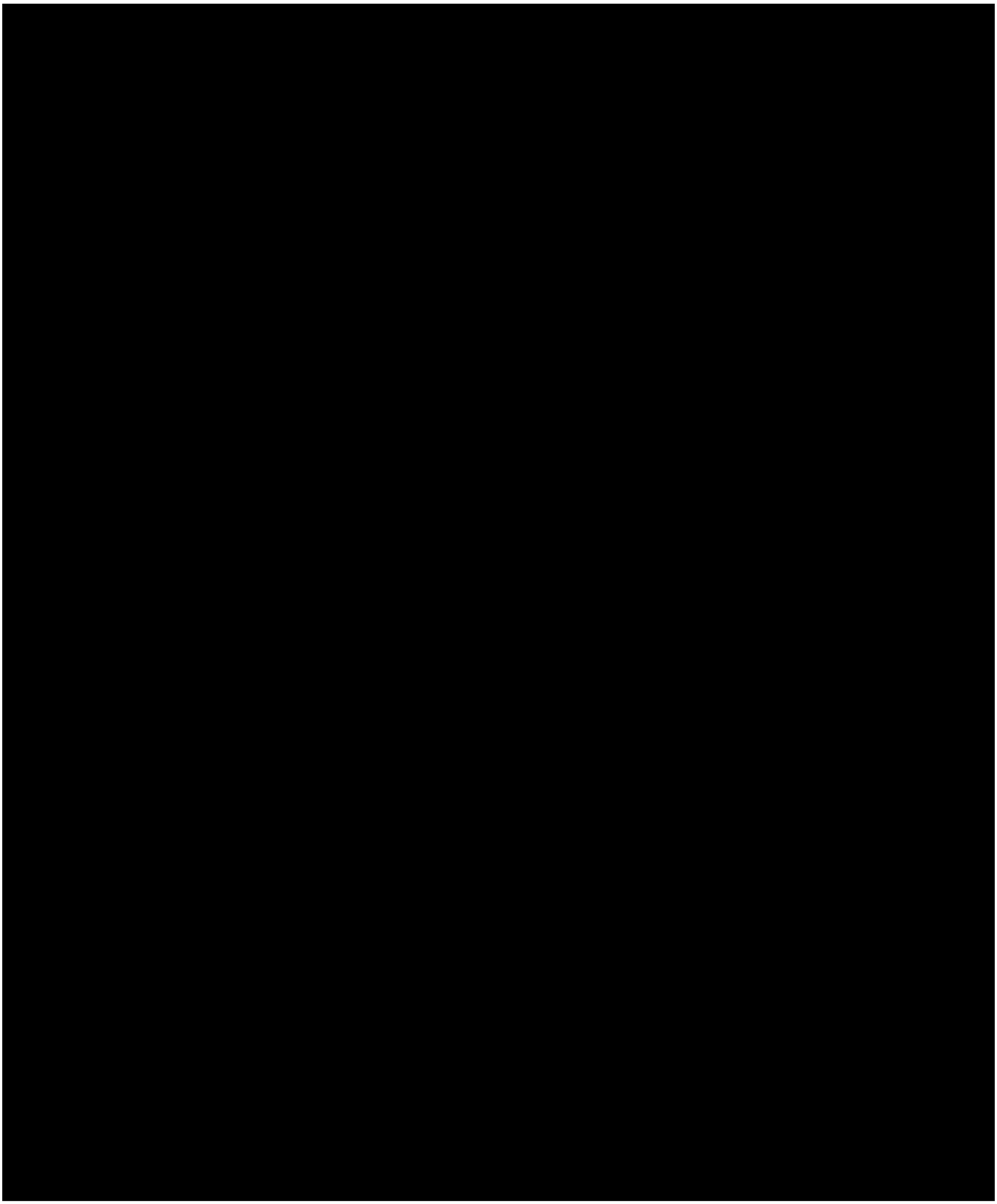


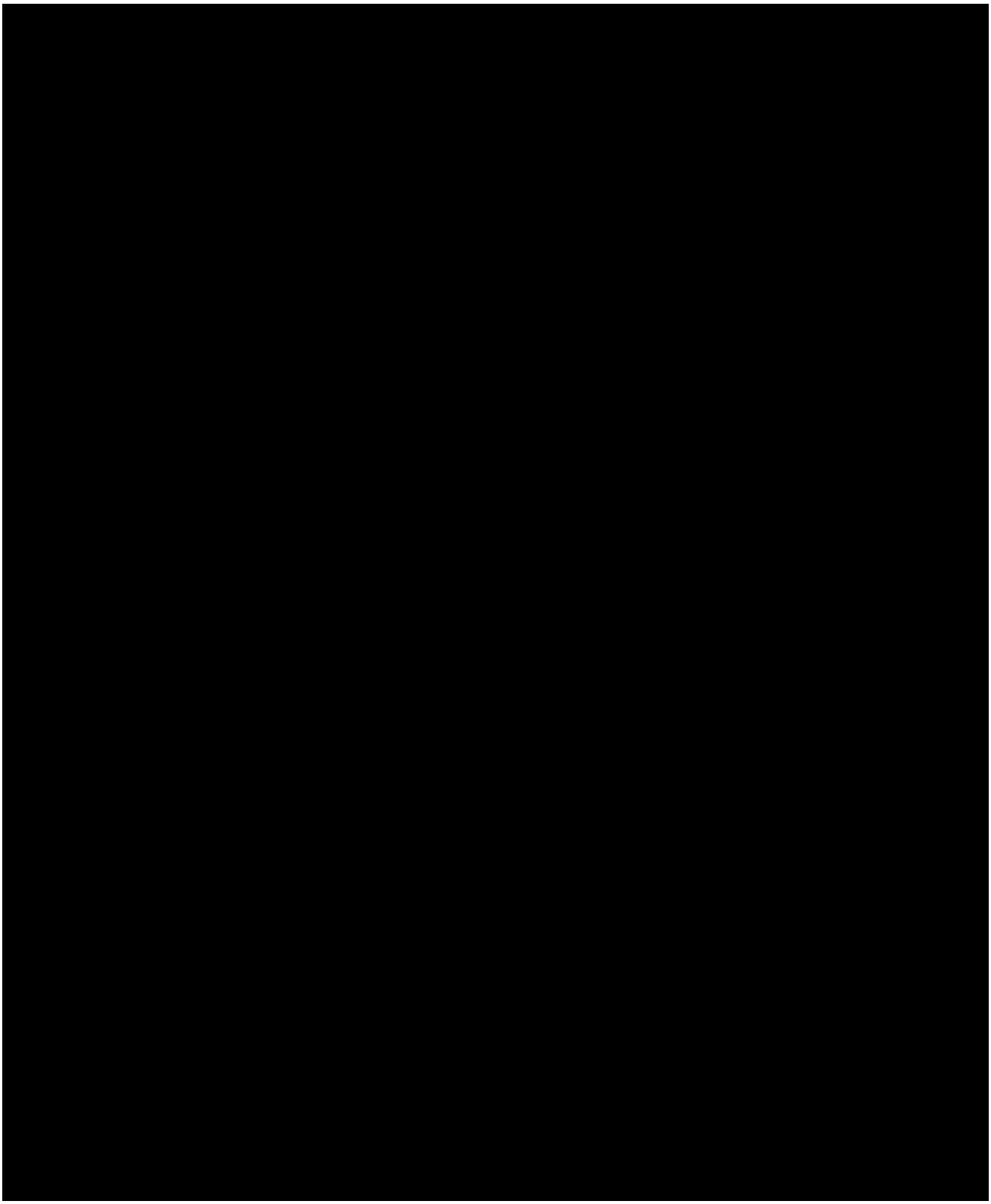


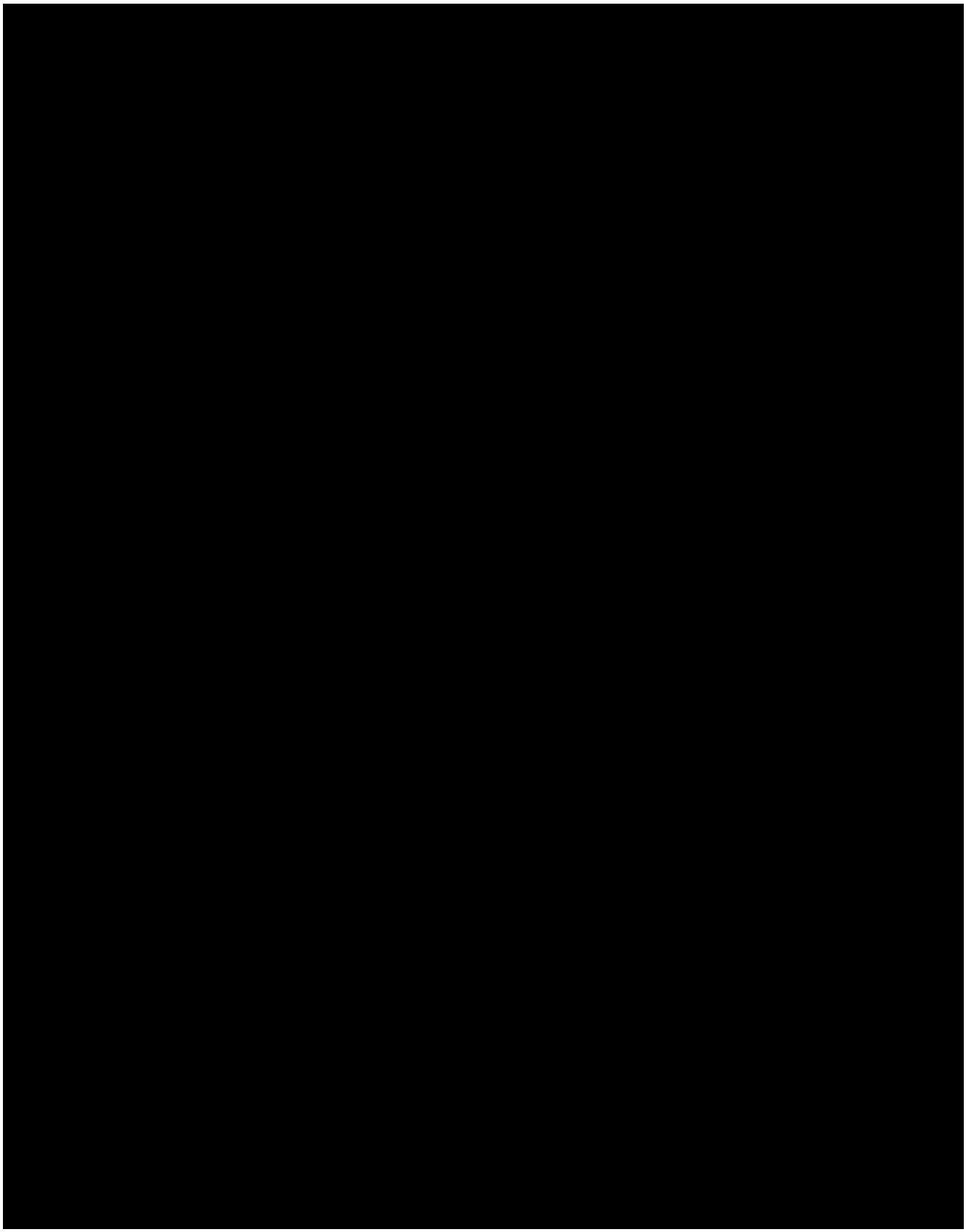


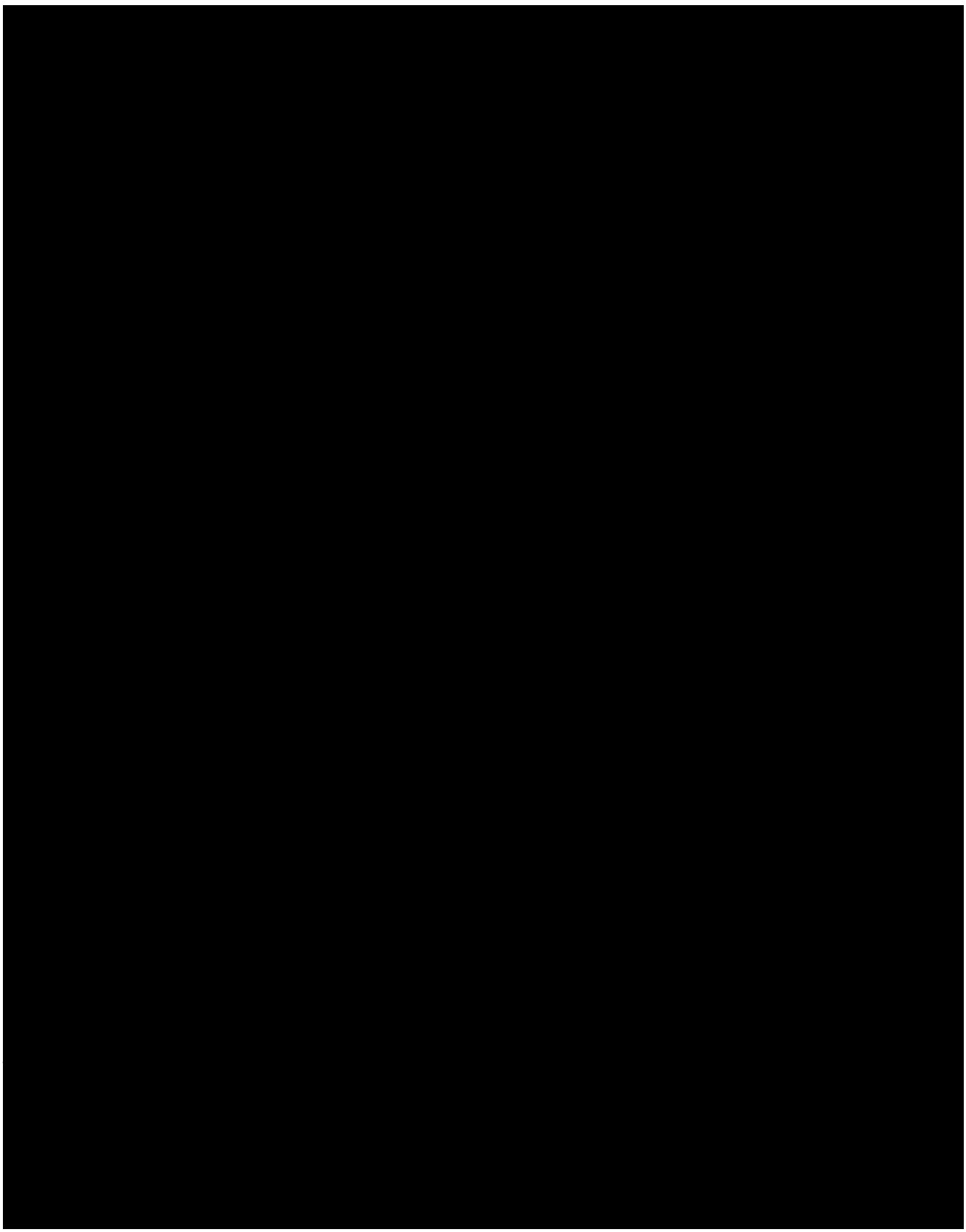


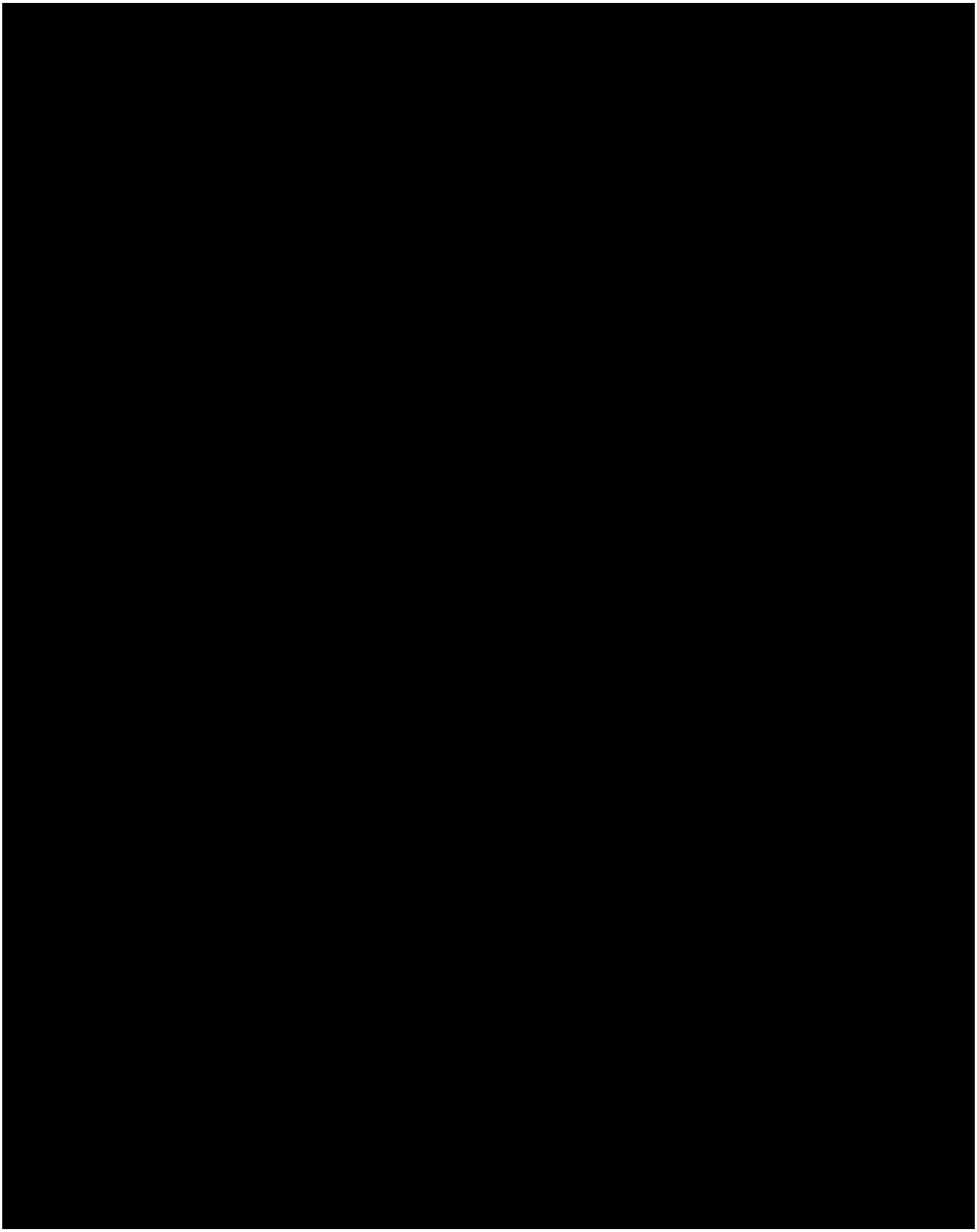


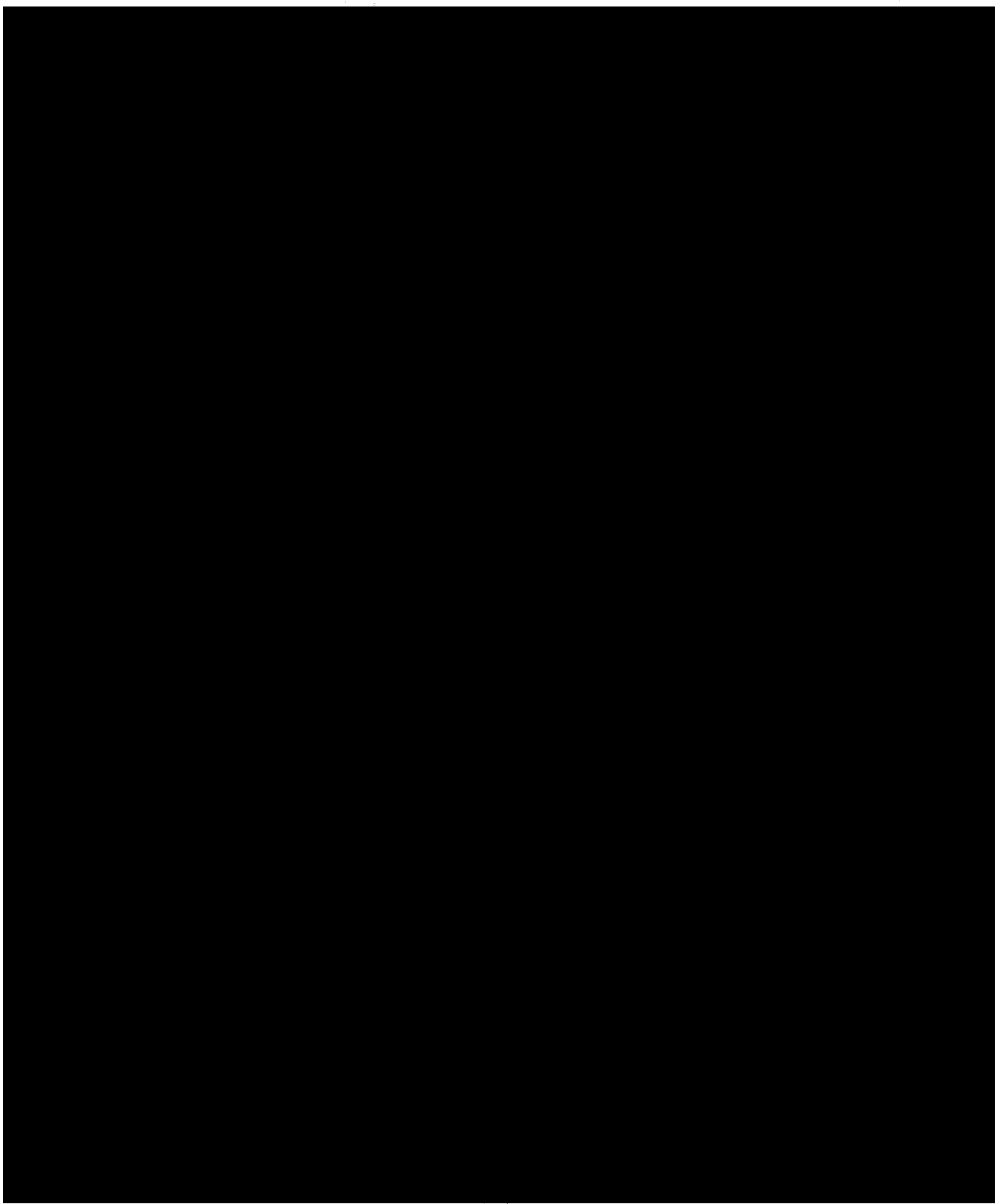


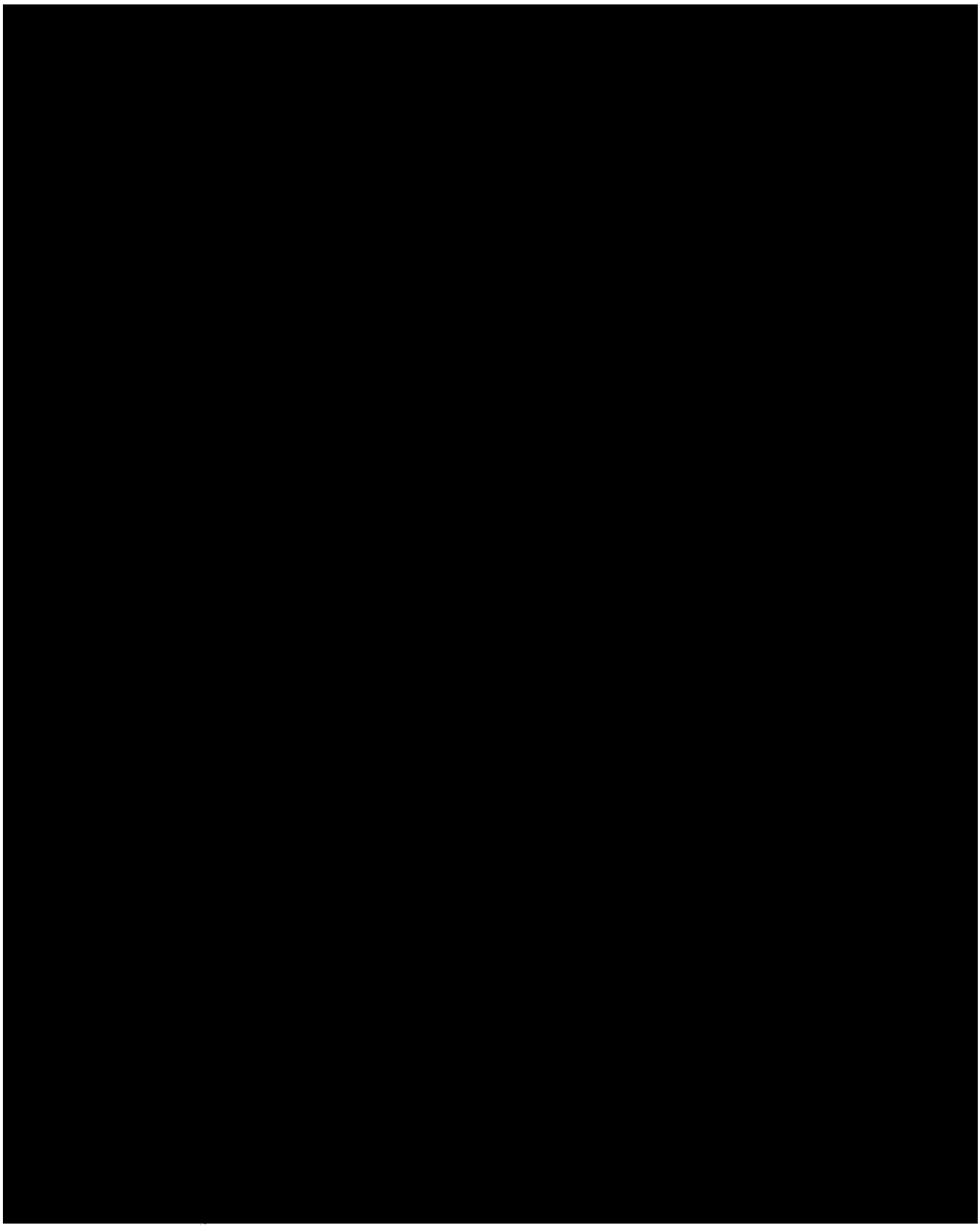


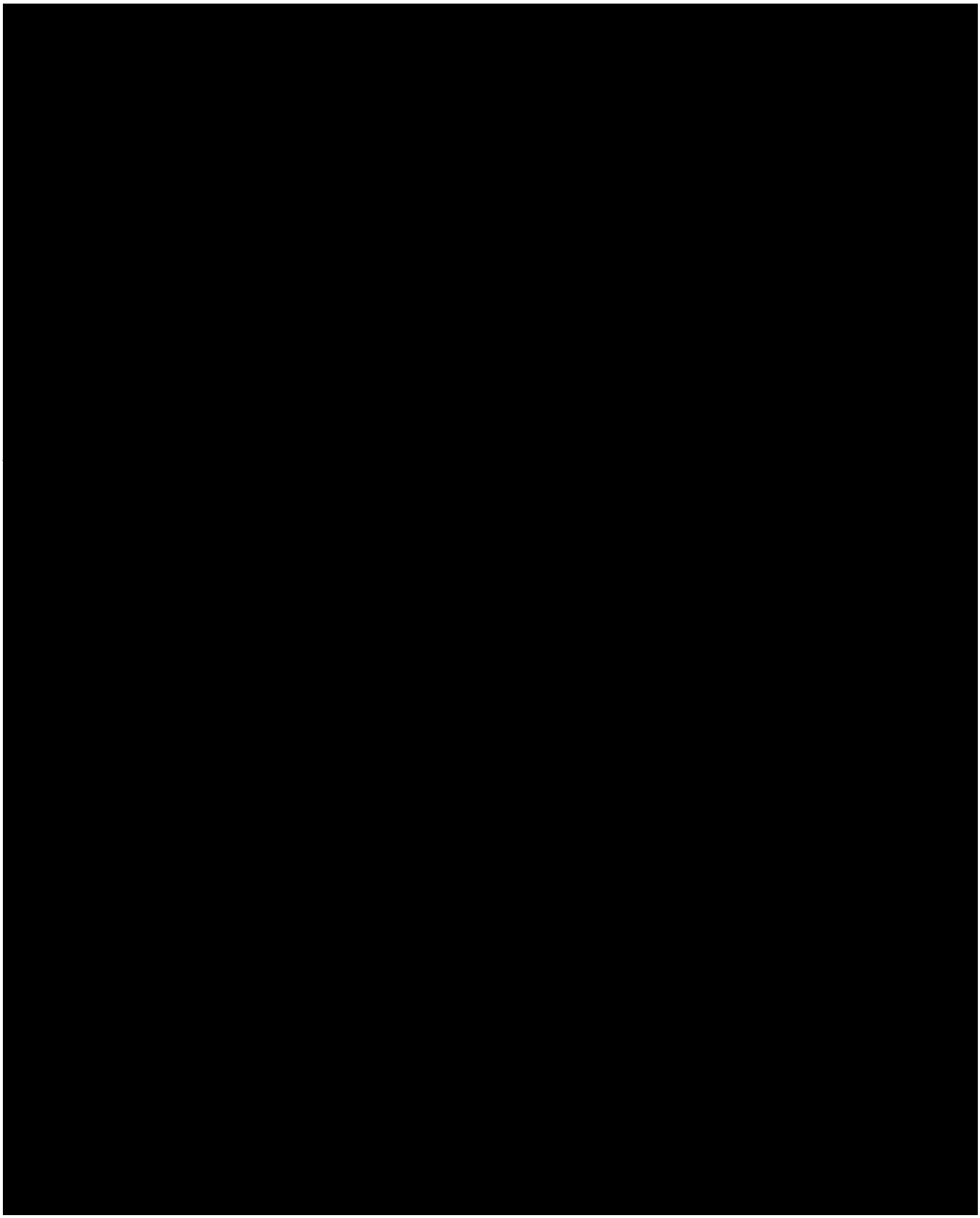












21 MAG 11317

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the [redacted]

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Apple Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Mary Jo Corkery of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the [redacted] contain evidence, fruits,

and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, flight from prosecution, and/or intimidation of potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of

this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

11/24/2021
Date Issued

9:32 a.m.
Time Issued

THE HONORABLE STEWART D. AARON
UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Apple Inc. (the "Provider"), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider's possession, custody, or control associated with the [redacted]

[redacted]

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary,

alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2018 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2018 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and

deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside technical experts or vendors under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) 18 U.S.C. §§ 201 and 371 (bribing or offering to bribe or demanding or accepting a bribe, and conspiring to do the same); (ii) 18 U.S.C. §§ 1343, 1346 and 1349 (honest services wire fraud and conspiring to commit honest services wire fraud); (iii) 18 U.S.C. § 1951 (extortion under color of right and conspiring to do the same); and (iv) 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in a financial transaction in criminally-derived property, and conspiracy to do the same) (collectively, the "Subject Offenses"), including the following:

- Communications between or involving one or more of Nadine Arslanian, Robert Menendez, Wael Hana, Jose Uribe, [redacted] and/or others, or photographs or other documents, regarding interactions between Hana, Uribe, [redacted] and [redacted], on the one hand, and Menendez or others acting on Menendez's behalf, on the other hand;
- Communications, photographs, or other documents or records concerning a New Jersey state criminal case against [redacted], including communications with or regarding the New

Jersey Attorney General's office, any attorney for [redacted], or any person acting at Menendez's direction to resolve that case or otherwise assist [redacted];

- Communications, photographs, or other documents or records concerning any official acts performed or requested to be performed by Menendez, or by Arslanian or anyone else acting or purporting to be acting in concert with Menendez—for the benefit of [redacted], Hana, Uribe, or [redacted], or of any persons acting on their behalf;
- Communications, photographs, or other documents or records concerning any gifts, services and/or money offered or provided to Arslanian and/or to Menendez by Hana, [redacted], Uribe, [redacted], or persons acting on their behalf, and/or receipt or solicitation of the same;
- Communications, photographs, or other documents or records concerning the location of evidence of any such gifts, services and/or money or concerning the location of any such gifts and/or money;
- Communications, photographs, or other documents or records concerning a potential disclosure of such gifts, services, and/or money;
- Communications, photographs, or other documents or records concerning a search warrant executed on or about November 25, 2019, including communications concerning a federal investigation involving Hana;
- Communications, photographs, or other documents or records concerning the use of alternative methods of communications believed to be less easily accessed or intercepted by law enforcement;

- Communications, photographs, documents, records, or other media evidencing the background and nature of the relationship between Menendez, Hana, Arslanian, Uribe, [redacted] and/or [redacted], or persons acting on their behalf;
- Information, including geolocation information, concerning the timing or location of communications or actions in furtherance of one or more of the Subject Offenses (*e.g.*, information that places Hana, Uribe, [redacted] Arslanian, Menendez, and/or others in particular locations or communicating at particular times and locations in connection with the Subject Offenses);
- Information concerning the identity of the user(s) of the Subject Accounts at times relevant to one or more of the Subject Offenses;
- Information concerning the identities and locations of co-conspirators (including, for example, communications with co-conspirators, photos or other attachments, and address book information); and
- Information concerning passwords or other information needed to access a user's computer, electronic devices or other online accounts used in furtherance of one or more of the Subject Offenses.

